ДАПАМОЖНІК
ДЛЯ БЛОГЕРАЎ

РЭПАРТЭРЫ БЯЗЬ МЕЖАЎ

ВЕРАСЕНЬ 2005

ДАПАМОЖНІК
ДЛЯ БЛОГЕРАЎ

РЭПАРТЭРЫ БЯЗЬ МЕЖАЎ

ВЕРАСЕНЬ 2005

ДАПАМОЖНІК

ДЛЯ БЛОГЕРАЎ

РЭПАРТЭРЫ БЯЗЬМЕЖАЎ

ЗЬМЕСТ

06 Блогеры – новыя вяшчальнікі свабоды
Жульен Пэйн (Julien Pain)

08 Што такое блог?
Pointblog.com

09 Мова блогінгу
Pointblog.com

12 Выбар інструмэнта
Сырыл Фэўе (Cyril Fievet), Марк Аліўе Пэйер (Mark-Olivier Peyer)

17 Як распачаць і весьці блог
The Civiblog system, Citizenlab

21 Якой павінная быць этыка блогера?
Дэн Гілмар (Dan Gillmor)

24 Што трэба зрабіць, каб блог заўважылі пошукавыя сыстэмы.
Аліўе Андрыё (Olivier Andrieu)

30 Што трэба зрабіць, каб блог "зазьзяў"?
Марк Глэйзер (Mark Glaser)

23 Асабісты вопыт

33 • **Нямеччына:** "Мы абараняем правы чалавека і грамадзянскія правы"
Маркус Бекедаль (Markus Beckedahl)

35 • **Бахрэйн:** "Мы зьнішчылі дзяржаўную манаполію на навіны"
Чанад Бахрэйні (Chan'ad Bahraini)

37 • **ЗША:** "Цяпер я магу пісаць тое, што думаю"
Джэй Роузэн (Jay Rosen)

41 • **Ганконг:** "Я выканала абяцаньне, дадзенае тым, хто загінуў"
Ян Шам-Шэклтан (Yan Sham-Shackleton)

43 • **Іран:** "У блогах мы можам пісаць свабодна"
Араш Сігарчы (Arash Sigarchi)

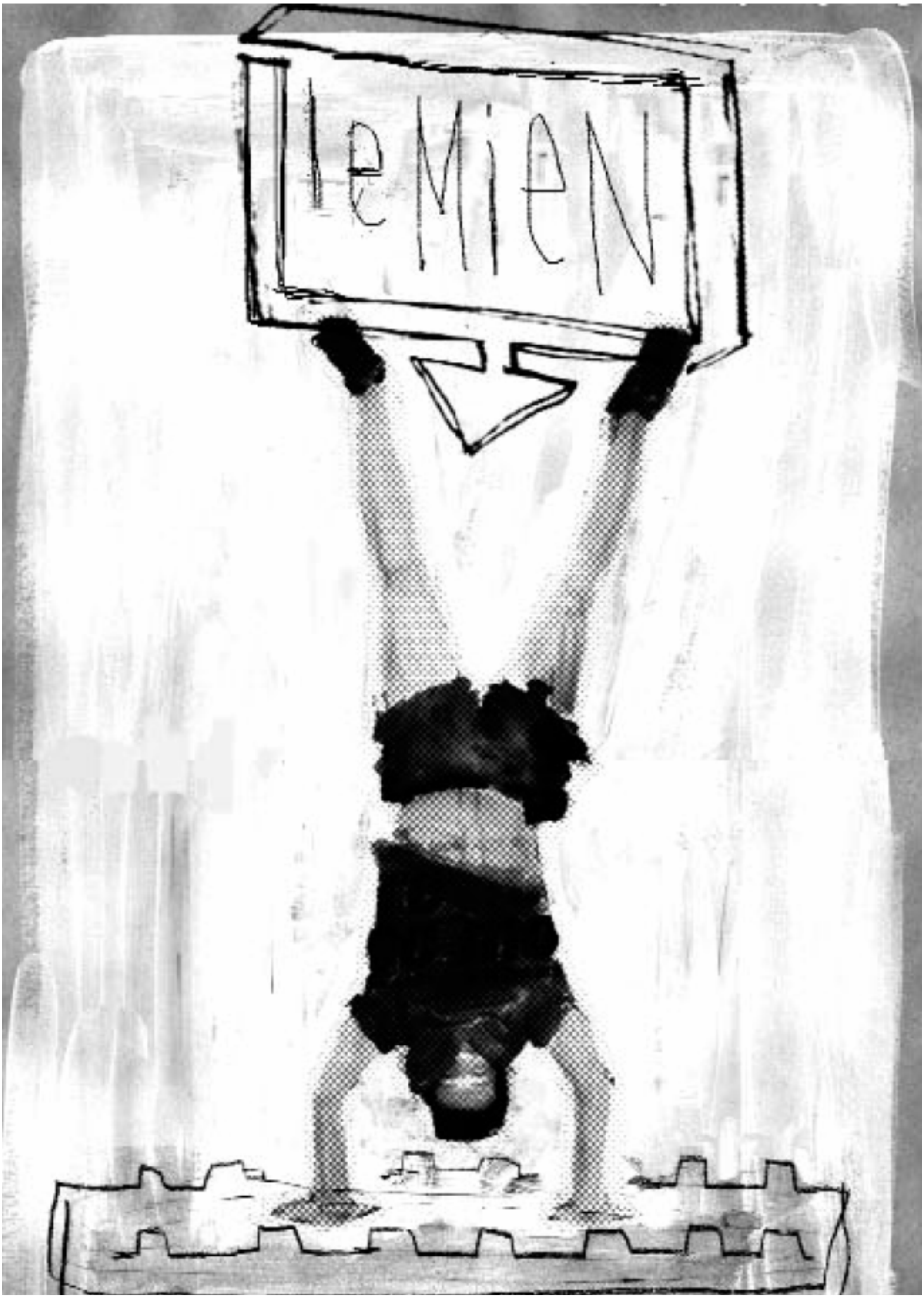
45 • **Нэпал:** "Мы распавядаем сьвету пра тое, што тут адбываецца"
Блог "Радыё "Свабодны Нэпал"

48 Як весьці блог ананімна
Этан Цукерман (Ethan Zuckerman)

55 Тэхнічныя парады, як абыйсьці цэнзуру
Нарт Віленёв (Nart Villeneuve)

69 Як забясьпечыць канфідэнцыйнасьць электроннага ліставаньня
Людовік Пьера (Ludovic Pierrat)

72 Чэмпіянат Сьвету па цэнзуры ў інтэрнэце
Жульен Пэйн (Julien Pain)


ІеМіеN

БЛОГЕРЫ, НОВЫЯ ВЯШЧАЛЬНІКІ СВАБОДЫ

Жульен Пэйн (Julien Pain)

У адных блогі выклікаюць захапленьне, іншых, наадварот, турбуюць, камусьці перашкаджаюць. Хтосьці ім не давярае, а хтосьці бачыць у блогах авангард новай інфармацыйнай рэвалюцыі. Відавочна адно – яны кідаюць выклік мэдыям у самых розных краінах, як, напрыклад, ЗША, Кітай ці Іран.

Яшчэ ня час выносіць ацэнку блогам. За тыя дзесяцігодзьдзі, што мы чытаем газэты, глядзім тэлебачаньне ды слухаем радыё, мы навучыліся імгненна адрозьніваць навіны ад камэнтароў, таблоідныя часопісы ад сур'ёзных і забаўляльныя перадачы ад дакумэнтальных фільмаў.

Але ў дачыненьні да блогаў мы яшчэ ня маем такіх выразных арыентыраў. Гэтыя "онлайнавыя дзёньнікі" нашмат больш разнастайныя, чым традыцыйныя мэдыі, і вельмі цяжка вызначыць, дзе сайт навінаў, а дзе асабісты форум, ці гэта сайт, прысьвечаны сур'ёзным дасьледаваньням, ці сайт з наборам бессэнсоўных фактаў. Цяжка аддзяліць пшаніцу ад саломы.

Некаторыя блогеры паступова выпрацоўваюць уласныя этычныя нормы, каб заваяваць давер чытачоў. Аднак у інтэрнэце ўсё яшчэ вельмі шмат ненадзейнай інфармацыі, шмат людзей абражаюць адзін аднаго. Блог дае магчымасьць кожнаму апублікаваць свой матэрыял, незалежна ад адукацыі ці тэхнічных навыкаў. Гэта значыць, што нудных ці агідных блогаў зьявіцца столькі ж, колькі добрых і цікавых.

Аднак блогінг – гэта магутны інструмэнт, які забясьпечвае свабоду слова. Ім ужо захапіліся мільёны простых людзей. Пасыўныя спажыўцы інфармацыі сталі энэргічнымі практыкамі новай журналістыкі, якую амэрыканскі піянэр блогінгу Дэн Гілмар назваў "народнай журналістыкай, якая робіцца людзьмі і для людзей" (гл. разьдзел "Этыка блогера").

Нярэдка блогеры зьяўлюцца адзінымі сапраўднымі журналістамі ў краінах, дзе традыцыйныя мэдыі патрапляюць пад цэнзуру ці пад іншы ціск. Толькі яны перадаюць незалежныя навіны, рызыкуючы выклікаць незадаволенасьць уладаў ці патрапіць пад арышт. Шмат якіх блогераў перасьледуюць ці кідаюць у турмы. Аднаго з аўтараў гэтай кнігі, Араша Сігарчы, прыгаварылі да чатырнаццаці гадоў турэмнага зьняволеньня за тое, што ён раьмясьціў у інтэрнэце тэксты з крытыкай іранскага рэжыму. Яго гісторыя сьведчыць пра тое, што шмат якія блогеры лічаць сваім абавязкам весьці блог. Для іх гэта неабходнасьць, а не хобі. Яны адчуваюць сябе вачыма і вушыма тысяч карыстальнікаў інтэрнэту.

Блогеру, які разьмяшчае рызыкоўную для сябе інфармацыю, трэба дзейнічаць ананімна. Кібэр-паліцыя ня сьпіць і вельмі ўдала адсочвае "парушальнікаў парадку". У гэтым дапаможніку Этан Цукерман навучыць вас, як разьмясьціць матэрыял і ня выдаць сябе (разьдзел "Як весьці блог ананімна"). Вядома ж, добра валодаць неабыходнымі тэхнічнымі навыкамі, каб дзейнічаць у сеціве ананімна, але часам можа дапамагчы і выкананьне некалькіх простых правілаў. Безумоўна, гэтыя парады не для тых, хто з дапамогай сеціва хоча зьдзейсьніць злачынства (тэрарысты, рэкеціры ці пэдафілы). Гэты дапаможнік мае сваёй мэтай дапамагчы блогерам, што апынуліся ў апазыцыі, таму што сваімі блогамі яны дэкляруюць свабоду слова.

Аднак бясьпека – не асноўная праблема блогера, нават пры рэпрэсіўным рэжыме. Праблема ў тым, каб зрабіць блог папулярным і знайсьці сваю аўдыторыю. Блог без чытачоў не прыцягне ўвагу кібэр-паліцыі, але які ў ім сэнс? Гэты дапаможнік дае тэхнічныя парады, як зрабіць, каб блог знайшлі асноўныя пошукавыя сыстэмы (артыкул Аліўе Андрыё), а таксама прапануе

некалькі адпаведных “журналісцкіх” прыёмаў (Што трэба зрабіць, каб блог “зазьзяў”, аўтар Марк Глэйзер).

Некаторыя блогеры сутыкаюцца з праблемай фільтрацыі. Сёньня большасьць аўтарытарных рэжымаў валодае тэхнічнымі магчымасьцямі для ажыцьцяўленьня цэнзуры інтэрнэту. На Кубе ці ў Віетнаме няма доступу да сайтаў, што крытыкуюць рэжым, выкрываюць карупцыю ці распавядаюць пра парушэньні правоў чалавека.
Так званы “незаконны” ці “падрыўны” зьмест аўтаматычна блякуецца фільтрамі. Але блогерам патрэбен вольны доступ да ўсіх сайтаў і да блогасфэры – інакш зьмест іх блогаў страчвае сэнс.

У другой частцы дапаможніка даюцца парады, як пазьбегнуць фільтрацыі (“Тэхнічныя парады, як абыйсьці цэнзуру”, аўтар Нарт Віленёв). Крыху здаровага розуму, упартасьць, і, што самае галоўнае, выбар правільных інструмэнтаў – і любы блогер здолее абыйсьці цэнзуру.

У дапаможніку зьмешчаныя тэхнічныя парады і падказкі, як зрабіць добры блог. Але нашмат больш складана стварыць пасьпяховы блог. Каб вас заўважылі, неабходна быць арыгінальным і прапаноўваць навіны ці меркаваньні, якія асноўныя медыі абыходзяць. У адных краінах блогеры заклапочаныя, перш за ўсё, тым, як не патрапіць у турму. У іншых яны імкнуцца заваяваць рэпутацыю крыніцы надзейнай інфармацыі. Ня ўсе блогеры маюць аднолькавыя праблемы, але ўсе яны , кожны сваёй хадой, крочаць у першых радах ваяроў за свабоду слова.

Жульен Пэйн – кіраўнік праекта “Свабода ў інтэрнэце” арганізацыі “Рэпартэры бязь межаў”.

ШТО ТАКОЕ БЛОГ?

Pointblog.com

“БЛОГ” ці “ЎЭБЛОГ” – асабістая старонка ў інтэрнэце, якая:

- зьмяшчае пераважна навіны (“posts”);
- рэгулярна абнаўляецца;
- вядзецца ў форме дзёньніка (апошнія запісы разьмяшчаюцца ў верхняй частцы старонкі), большасьць матэрыялаў падзяляецца на рубрыкі;
- запускаецца з дапамогай адмысловых інтэрактыўных інструмэнтаў;
- звычайна ствараецца і вядзецца адным чалавекам, часам ананімна.

НАТАТКІ БЛОГА (POSTS):

- звычайна гэта тэкст (са зьнешнімі спасылкамі), часам у гукавым ці відэа-суправаджэньні, што апошнім часам сустракаецца ўсё часьцей;
- могуць камэнтавацца наведвальнікамі;
- архівуюцца на блогу, маюць неабмежаваны доступ.

ТАКІМ ЧЫНАМ, БЛОГ ШМАТ У ЧЫМ ПАДОБНЫ ДА “АСАБІСТАЙ УЭБ-СТАРОНКІ”, АЛЕ БЛОГ:

- лягчэй стварыць і падтрымліваць, таму ён болей дынамічны і часьцей абнаўляецца;
- патрабуе больш адкрытага і асабістага стылю, больш шчырага выказваньня думак;
- заахвочвае да дыскусій наведнікаў ды іншых блогераў;
- мае фармат міжнароднага стандарту для блогаў, у тым ліку, больш-менш аднолькавую структуру (тэкст арганізаваны ў дзьве-тры калонкі, з камэнтарамі і RSS (really simple syndication) каналам.

МОВА БЛОГІНГУ

Pointblog.com

БЛОГ (BLOG)
Скарачэньне ад "уэблог". Сайт, які зьмяшчае пісьмовыя матэрыялы, спасылкі ці фотаздымкі, якія стала абнаўляюцца, звычайна адным чалавекам.

ВЕСЬЦІ БЛОГ (TO BLOG)
Весьці блог, разьмяшчаць матэрыял на блогу.

БЛОГЕР (BLOGGER)
Чалавек, які вядзе блог.

БЛОГАСФЭРА (BLOGOSPHERE)
Усе блогі, супольнасьць блогераў

СЬПІС СПАСЫЛАК (BLOGROLL)
Сьпіс зьнешніх спасылак, што разьмяшчаюцца на блогу. Часта гэта лінкі (спасылкі) на іншыя блогі, звычайна разьмешчаныя ў калонцы на хатняй старонцы. Нярэдка гэта спасылкі на "суполку" блогераў-сяброў.

КАМЭНТАРЫ-СПАМ (COMMENT SPAM)
Тое ж, што і спам у электроннай пошце. Робаты ("spambots") дасылаюць на блог рэкляму ў выглядзе псэўда-камэнтараў. Гэта сур'ёзная праблема, якая патрабуе ад блогераў і блогавых плятформаў выкарыстаньня адмысловых праграм, каб зачыніць доступ для некаторых карыстальнікаў або забараніць некаторыя адрасы ў камэнтарах.

СЫНДЫКАЦЫЯ ЗЬМЕСТУ (CONTENT SYNDICATION)
Спосабы, з дапамогай якіх аўтар ці адміністратар сайта робяць матэрыялы свайго сайта альбо іх часткі даступнымі для разьмяшчэньня на іншых уэб-сайтах.

МОБЛОГ (MOBLOG)
Скарачэньне ад "мабільны блог" ("mobile blog"). Блог, які можа абнаўляцца дыстанцыйна, з выкарыстаньнем такіх сродкаў камунікацыі, як тэлефон ці лічбавы асыстэнт.

СТАЛАЯ СПАСЫЛКА, ПЭРМАЛІНК (PERMALINK)
Скарачэньне ад "сталая спасылка" ("permanent link"). Уэб-адрас кожнага матэрыялу, разьмешчанага на блогу. Зручная закладка, нават у выпадках, калі матэрыял заархіваваны на блогу, зь якога быў узяты.

ФОТАБЛОГ (PHOTOBLOG)
Блог, які зьмяшчае пераважна фотаздымкі ў храналагічнай пасьлядоўнасьці і ўвесь час абнаўляецца.

ПАДКАСТЫНГ (PODCASTING)
Скарачэньне ад "iPod" і "broadcasting"(вяшчаньне). Разьмяшчэньне аўдыё- і відэаматэрыялаў на блогу і яго RSS канале для лічбавых плэераў.

НАТАТКА (POST)
Звычайна кароткае паведамленьне, разьмешчанае на блогу, суправаджаецца зьнешняй спасылкай, наведнікі могуць яго камэнтаваць. Гэта могуць быць навіны, фотаздымкі ці проста спасылкі.

RSS (REALLY SIMPLE SYNDICATION/ САПРАЎДЫ ПРОСТАЯ СЫНДЫКАЦЫЯ)
Спосаб абыходжаньня з апошнімі паведамленьнямі, разьмешчанымі на ўэб-сайце. Асабліва зручны для блогаў, таму што паведамляе карыстальнікам пра кожнае абнаўленьне іх улюбёных блогаў. Таксама можа "сындыкаваць" зьмесьціва, дазваляючы іншым сайтам (проста і аўтаматычна) перадаваць усё зьмесьціва нейкага сайта ці яго частку. Хутка распаўсюджваецца, асабліва на сайтах сродкаў масавай інфармацыі.

RSS АГРЭГАТАР (RSS AGGREGATOR)
Праграмнае забясьпечаньне альбо онлайнавая паслуга, якая дазваляе блогеру чытаць RSS канал (RSS feed), асабліва апошнія паведамленьні на яго ўлюбёных блогах.

Агрэгатар таксама называюць “чытальнікам” (reader) ці “чытальнікам канала” (feedreader).

RSS КАНАЛ (RSS FEED)
Файл, які зьмяшчае апошнія нататкі на блогу. Ён счытваецца RSS агрэгатарам/ чытальнікам (RSS aggregator/reader) і адразу ж паказвае абнаўленьне блога.

ЗВАРОТНАЯ СПАСЫЛКА (TRACKBACK)
Спосаб аўтаматычнай сувязі паміж сайтамі, калі яны абменьваюцца паведамленьнямі пра тое, што на блогу зьявілася інфармацыя, зьвязаная з папярэдняй нататкай (post).

УЭБ- ДЗЁНЬНІК (WEB DIARY)
Блог.

ВІКІ (WIKI)
Гавайскае “wikiwiki” – “хуткі”. Уэб-сайт, які можа лёгка і хутка абнаўляцца любым наведнікам. Гэтым словам таксама пачалі называць інструмэнты, якія выкарыстоўваюцца для стварэньня вікі (вікі рухавікі). Блогі і вікі ў нечым падобныя, але гэта не адно і тое ж.

ВЫБАР **ІНСТРУМЭНТА**

Сырыл Фэўе (Cyril Fievet), Марк Аліўе Пэйер (Mark-Olivier Peyer), pointblog.com

Блогі шмат у чым абавязаныя разьвіцьцю праграмаў, што аблягчаюць працэс абнаўленьня ўэб-старонак.
Праграмныя інструмэнты для вядзеньня блога павінныя забясьпечваць, перш за ўсё, зручны для карыстальніка інтэрфэйс (даступны праз уэб-браўзэр), а таксама дынамічна кіраваць зьмесьцівам з дапамогай архіваў і пошуку.

Блог мае два адрасы ў сеціве, якія застаюцца нязьменнымі пасьля запуску блога:
- адрас для грамадзкага доступу;
- адміністрацыйны адрас, абаронены паролем, які належыць чалавеку, што вядзе блог.

Блог можна ўсталяваць, далучыўшыся да блог-супольнасьці ці на сваім сэрвэры.

БЛОГ-СУПОЛЬНАСЬЦІ

(Гл. разьдзел "Як распачаць і весьці блог", The Cibviblog system)
Усталяваньне блога праз далучэньне да ўжо існуючай супольнасьці звычайна займае некалькі хвілін. Выбіраеце імя карыстальніка і пароль, некалькі разоў "клікаеце" - і блог запушчаны. Адныя блог-супольнасьці бяруць за гэта грошы, іншыя – не.
Такі спосаб прыймальны, калі вы хочаце стварыць блог "толькі для прагляду": каштуе няшмат (максімум некалькі эўра на месяц), усё проста і хутка. Акрамя таго, вы маеце выгоды ад трафіку, які гэнэруецца супольнасьцю, а таксама з таго, што суполка ўжо добра вядомая. Сярод нязручнасьцяў – абмежаваныя магчымасьці для стварэньня інтэрфэйса і больш прасунутых характарыстык, а таксама неабходнасьць разьмяшчаць рэкляму. Таксама існуе пагроза, што супольнасьць зачыніцца.

Выбар інструмэнта

САМАСТОЙНАЕ ВЫКАРЫСТАНЬНЕ ПРАГРАМНАГА ЗАБЕСЬПЯЧЭНЬНЯ ДЛЯ БЛОГІНГУ

Інструмэнты блогінгу - гэта праграмы, якія ўсталёўваюцца на сэрвэры з выкарыстаньнем script-праграм для аўтаматычнага запуску сайтаў і базы дадзеных для захоўваньня разьмешчаных матэрыялаў.Пасьля ўсталяваньня гэтыя праграмы працуюць праз стандартны ўэб-навігатар. Пры гэтым, для ўстаноўкі і запуску блога не патрэбныя нейкія спэцыяльныя веды, напрыклад, веданьне HTML. Аднак інсталяцыя і выбар канфігурацый (выбар крытэраў доступу, стварэньне базы дадзеных, падрыхтоўка FTP-загрузкі (FTP-loading) могуць уяўляць сабой некаторыя цяжкасьці.

Такое рашэньне падыходзіць для тых, хто ўжо знаёмы з блогамі. Асноўная перавага гэтага спосабу ў тым, што блог належыць толькі вам; вы можаце без абмежаваньняў адаптаваць праграму да вашых патрэбаў ці задаваць новыя парамэтры. Аднак для гэтага патрэбныя некаторыя тэхнічныя навыкі. Акрамя таго, такі блог горш абаронены ад спам-камэнтараў, зьмесьціва вам таксама трэба будзе захоўваць самастойна.

ЯК ВЫБРАЦЬ БЛОГ-СУПОЛЬНАСЬЦЬ?

Часам пераход ад адной блог-супольнасьці да іншай можа ўяўляць сабой некаторыя цяжкасьці. Таму важна з самага пачатку зрабіць правільны выбар.

Пры выбары блог-супольнасьці неабходна ўлічваць наступныя моманты:
ШТО ЗА БЛОГІ Ў СУПОЛЬНАСЬЦІ

Некаторыя суполкі аб'ядноўваюць карыстальнікаў аднаго ўзросту ці людзей з аднолькавымі інтарэсамі. Прагледзьце некалькі дзесяткаў блогаў супольнасьці, каб вызначыць "тыповую" групу.

ЯК БЛОГ ВЫГЛЯДАЕ

Нягледзячы на тое, што звычайна выбар невялікі, старонкі супольнасьцяў (плятформаў) усё ж адрозьніваюцца колерамі, шрыфтамі і інтэрфэйсамі. Каб атрымаць уяўленьне пра гэтыя магчымасьці, прагледзьце некалькі блогаў. Многія супольнасьці з вольным уступам патрабуюць, каб блогеры разьмяшчалі рэкляму на ўсіх старонках. Зьвярніце ўвагу на тое, як выглядаюць адрасы. Прыклады: http://myblog.thecommunity.com, http://www.thecommunity.com/myblog ці http://www.thecommunity.com/mynumber).

МАГЧЫМАСЬЦІ

Прагледзьце прапанаваныя характарыстыкі і высьветліце, ці зможаце вы зьмяняць дызайн блога, запрашаць іншых аўтараў, разьмяшчаць выявы ці гукавыя файлы, ці магчыма абнаўленьне праз тэлефон. Вывучыце магчымасьці абмежаваньня доступу (поўнага ці частковага) для зарэгістраваных карыстальнікаў.

СХАВАНЫЯ ВЫДАТКІ

Некаторыя суполкі прапануюць бясплатныя паслугі, аднак калі аб'ём захаваных дадзеных дасягае пэўных памераў, а таксама за пэўную прапускную здольнасьць, можа патрабавацца аплата.
Гэта неабходна высьветліць загадзя.

МІЖНАРОДНЫЯ ПЛЯТФОРМЫ

Blogger – http://www.blogger.com
Бясплатная плятформа. Створаная ў 1999 годзе, купленая Google у 2003 годзе. Гэта самая буйная супольнасьць, у склад якой уваходзіць каля васьмі мільёнаў блогаў. Карыстацца плятформай проста, аднак яна мае абмежаваныя магчымасьці.

LiveJournal – http://www.livejournal.com
Бясплатная ці платная (каля 2 даляраў ЗША на месяц). Адна з найстарэйшах плятформаў, шэсьць мільёнаў блогаў, асноўныя карыстальнікі – моладзь.

MSN Spaces – http://www.msnspaces.com
Бясплатная. Плятформа Microsoft, створаная напрыканцы 2004 году. Шмат магчымасьцяў (абмен фотаздымкамі, Messenger link). Зарэгістравацца могуць толькі тыя, каму споўнілася 13 год.

ФРАНКАМОЎНЫЯ ПЛЯТФОРМЫ

20six – http://20six.fr
Бясплатная ці платная (3-7 эўра на месяц).Шмат магчымасьцяў, мае базавую і прасунутую вэрсіі.

Over-Blog – http://www.over-blog.com
Бясплатная. Добры дызайн, простая ў карыстаньні.

Skyblog – http://www.skyblog.com
Бясплатная (з абавязковай рэклямай). Найбуйнейшая плятформа ў Францыі, вельмі папулярная сярод моладзі, нягледзячы на абмежаваныя магчымасьці.

TypePad – http://www.typepad.com/sitefr

Платная (ад 5 да 15 эўра на месяц у залежнасьці ад характарыстык). Вельмі прафэсійная, з шырокім выбарам магчымасьцяў. Бясплатную вэрсію можна прыдбаць праз блог-супольнасьці, заснаваныя трэцяй стараной, напрыклад, Noos (http://www.noosblog.fr) ці Neuf Telecom (http://www.neufblog.com).

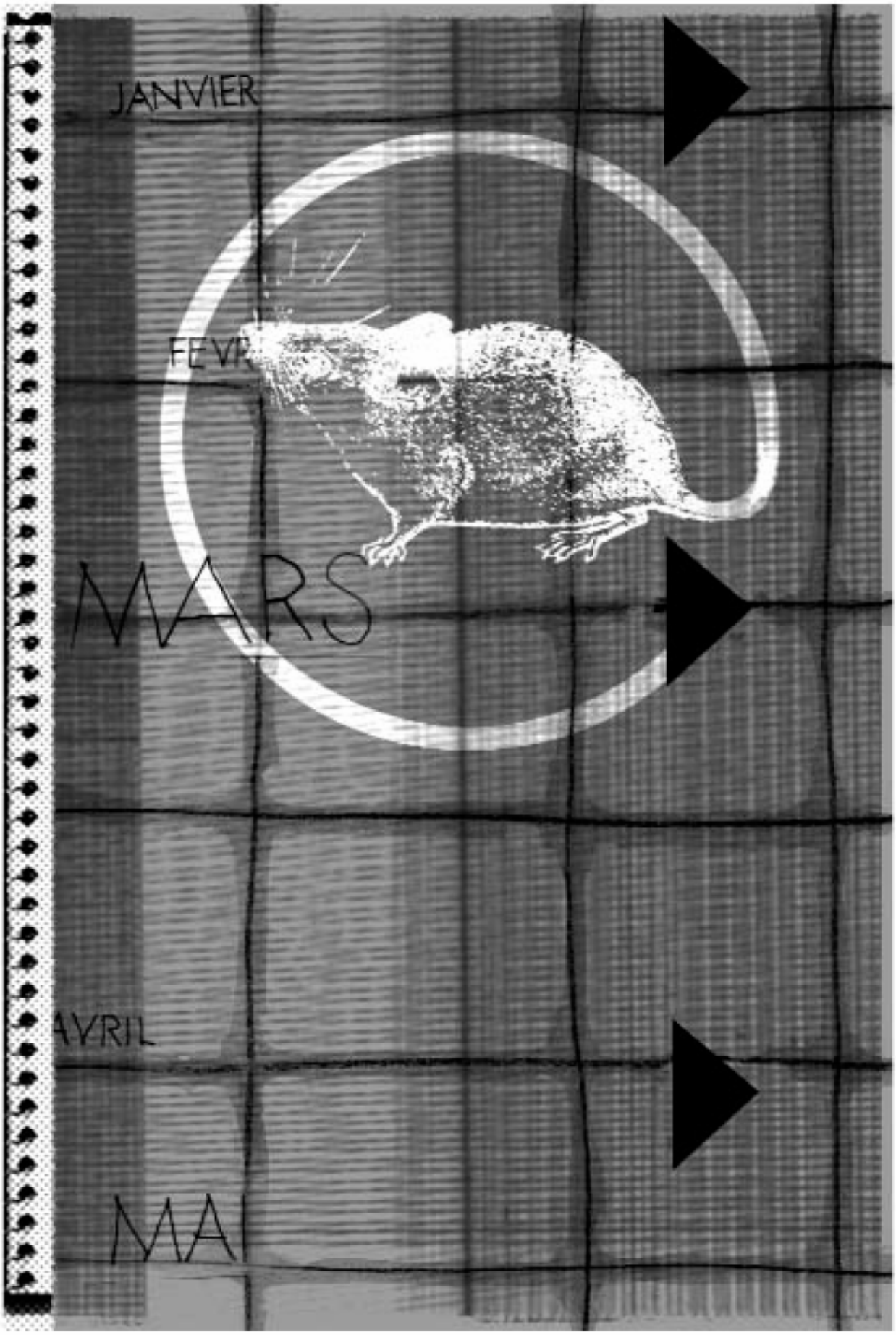
ViaBloga – http://viabloga.com
Бясплатная для НДА, у астатніх выпадках – 5 эўра на месяц . Арыгінальная, дынамічная, зь цікавымі магчымасьцямі.

ПРАГРАМНАЕ ЗАБЕСЬПЯЧЭНЬНЕ БЛОГАЎ

DotClear – http://www.dotclear.net
MovableType – http://www.movabletype.org
Wordpress – http://www.wordpress.org

Мэта Pointblog.com – асьвятляць сутнасьць і разьвіцьцё блогінгу як элемента сучаснай інтэрнэт-рэвалюцыі. Сайт прызначаны як для навічкоў, так і для вопытных карыстальнікаў, а таксама для наведнікаў. Складаецца з блогу і некалькіх асобных разьдзелаў. Блог вядзе кампанія Pointblog SARL, заснавальнікамі і кіраўнікамі якой зьяўляюцца Крыстоф Джынісьці (Chtistophe Ginisty) і Сырыл Фэўе (Cyril Fievet).

Мой блог


JANVIER
FEVR
MARS
AVRIL
MAI

ЯК **РАСПАЧАЦЬ І ВЕСЬЦІ** БЛОГ

Civiblog system (www.civiblog.org)

Блог нашмат лягчэй падтрымліваць і абнаўляць, чым звычайны ўэб-сайт. Блогавыя плятформы (ці сэрвэры) маюць у нечым адрозныя мэтады постынгу, але прынцыпы тыя ж самыя.

Мэта гэтага артыкула – дапамагчы карыстальнікам плятформы Civiblog, якая выкарыстоўваецца прадстаўнікамі грамадзянскай супольнасьці ва ўсім сьвеце, але парады тычацца і іншых падобных сэрвэраў. Civiblog выкарыстоўвае плятформу Blogware, якой кампанія Tucows дазволіла карыстацца бясплатна.

Перш за ўсё, зьвернем увагу на тое, дзякуючы чаму блогінг зрабіўся такім папулярным.

Першы тэхнічны ключ да благасфэры – гэта RSS (Really Simple Syndication) каналы. Базавым элемэнтам RSS зьяўляецца XML (eXtensible Markup Language) файл, які аўтаматычна гэнэруецца блогам, і на які іншы ўэб-сайт ці блог можа даць спасылку (link). Калі вы "сындыкуеце" RSS канал, ён разьмяшчае загалоўкі матэрыялаў блога ў вашым чыальніку навінаў (news reader) (у такіх паштовых праграмах, як Outlook і Thunderbird) альбо непасрэдна на вашым сайце ці блогу. Адначасова з абнаўленьнем блогу абнаўляецца і RSS канал. Дзякуючы гэтаму інфармацыя распаўсюджваецца аўтаматычна і хутка. Блогерам неабходна авалодаць гэтай тэхналёгіяй, каб сваечасова абнаўляць матэрыял.

Другі тэхнічны ключ да блогінгу – гэта зваротныя спасылкі (trackbacks), якія паказваюць паходжаньне матэрыяла на блогу і выкарыстоўваюцца большасьцю плятформаў.

Калі матэрыял, разьмешчаны на дадзеным блогу, узяты зь іншага блогу ці заснаваны на матэрыяле зь іншага блогу, можна дабавіць зваротную спасылку, каб аўтаматычна зрабіць запыт аб пераліку ўсіх сайтаў, паведамленьні зь якіх ці камэнтары да якіх разьмешчаныя на дадзеным сайце. Гэта гучыць складана, але насамрэч усё вельмі проста і дае вялікі плён. Згадзіцеся, заўсёды прыемна даведацца, што хтосьці зьвяртаецца да вашых матэрыялаў. Карысна і тое, што зьяўляецца магчымасьць папулярызаваць свой блог, а таксама гэнэраваць дыскусыі паміж блогамі.

Такім чынам, перш чым распачаць свой блог, азнаёмцеся з гэтай тэхналёгіяй.

ХАТНЯЯ СТАРОНКА CIVIBLOG
RSS канал разьмешчаны з правага боку і аўтаматычна абнаўляецца, як толькі сайт-чалец супольнасьці разьмяшчае новы матэрыял.

РЭГІСТРАЦЫЯ

Перш чым распачаць блог, неабходна зарэгістравацца. На большасьці плятформаў гэта робіцца вельмі проста. Civiblog патрабуе толькі нейкую асноўную інфармацыю, але ўсё адно правярае, ці насамрэч зарэгістраваныя на гэтай плятформе блогі вядуць прадстаўнікі грамадзянскай супольнасьці, што гэта не проста сямейныя блогі ці блогі для сяброў. Блог зьяўляецца онлайн прыкладна праз 24 гадзіны ад моманту рэгістрацыі. Коды доступу для запуску блога дасылаюцца блогеру па электроннай пошце.

УВАХОД У СЫСТЭМУ ДЛЯ АДМІНІСТРАТАРА

Блог мае "зьнешні інтэрфэйс" ("front end" – старонка, на якую прыходзяць наведнікі) і прыкладную частку ("back end"), адкуль блог абнаўляецца і вядзецца, а таксама апрацоўваюцца матэрыялы. Прыкаладная частка даступная праз імя карыстальніка і пароль, атрыманыя пры рэгістрацыі.

ПАНЭЛЬ НАСТРОЕК (DASHBOARD)

Большасьць блогераў мае "панэль настроек" ("dashboard"), якая дазваляе бачыць усё, што адбываецца на блогу, у тым ліку, апошнія нататкі, камэнтары, а таксама зваротныя спасылкі. Адсюль можна атрымаць доступ да ўсіх магчымасьцяў блога, зьмяняць яго выгляд, павялічваць прапускную здольнасьць, рэдагаваць ранейшыя нататкі, а таксама кіраваць доступам наведнікаў, напрыклад, дазваляць ім рабіць камэнтары, ці не.

ЯК РАЗЬМЯШЧАЦЬ ПАВЕДАМЛЕНЬНІ

Адно з асноўных адрозьненьняў блога ад звычайнай уэб-старонкі - гэта тое, што блог лягчэй абнаўляецца. Большасьць плятформаў дазваляе разьмяшчаць паведамленьні ў простым тэкставым фармаце. Новыя плятформы, такія, як Civiblog, дазваляюць зьмяняць памер і колер шрыфту, устаўляць спасылкі ды малюнкі.

Для разьмяшчэньня нататкаў неабходна:

1. Увайсьці ў сыстэму
2. Націснуць на "post" ("разьмясьціць")

3. Надрукаваць назву тэкста і сам тэкст
4. Адфарматаваць тэкст з дапамогай інтэрфэйса
5. Занесьці нататкі ў адну з наяўных рубрык ці стварыць новую рубрыку.
6. Націснуць "save" ("захаваць") унізе старонкі.

Вось і ўсё. Крыху вопыту, і вы зможаце пачаць карыстацца і іншымі інструмэнтамі, такімі, як, зваротныя спасылкі ("trackbacks"), пінгі ("pings") ці ключавыя словы ("keywords").

ЗВАРОТНЫЯ СПАСЫЛКІ (TRACKBACKS)

Дабавіць зваротную спасылку да нататкаў даволі проста. Вы проста дабаўляеце ў акно "trackback URLs to notify" сталы URL сайта, на які спасылаецеся. Зваротная ссылка будзе аўтаматычна дасланая на сайт адначасова з захаваньнем нататкаў.

RSS СЫНДЫКАЦЫЯ (RSS SYNDICATION)

Сындыкаваць RSS канал іншага сайта ці блога таксама даволі проста:

1. Увайдзіце ў "настройкі" ("back end") блога.
2. Націсьніце кнопку "улюбёнае" ("favourities").
3. "Клікніце" на "RSS headline components". ("кампанэнты RSS–загалоўкаў)
4. У адпаведнасьці з інструкцыямі ўстаўце URL (які сканчаецца на .xml, .rdf, альбо .py ці .php) RSS канала, які вы хочаце сындыкаваць.
5. Дайце каналу імя і націсьніце на "дабавіць канал" ("add feed").
6. Створаны канал устаўце ў блог.
7. Націсьніце на "look and feel" ("праверка").
8. Націсьніце на "layout" ("разьмяшчэньне").
9. Націсьніце на "RSS: your feed" ("ваш RSS канал") ("your feed" – гэта імя, якое вы прысвоілі каналу ў кроку 5. Цягніце назву канала на тое месца, дзе яна будзе знаходзіцца на блогу.
10. Націсьніце на "save" ("захаваць") унізе старонкі.

Вось і ўсё.

Вось некаторыя з мноства сайтаў, на якіх можна знайсьці карысную інфармацыю па блогінгу:

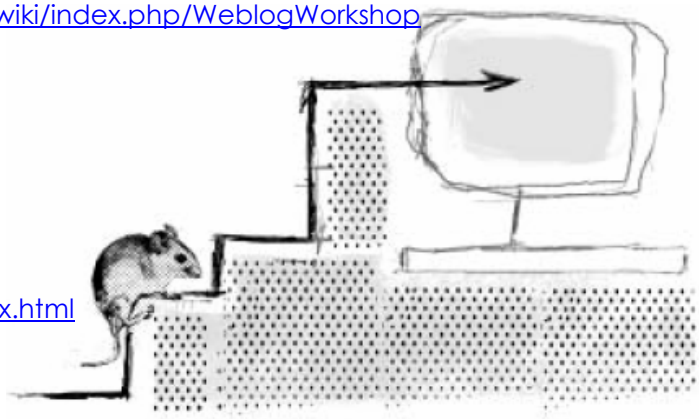
Civiblog Central Resources Blog:
http://central.civiblog.org/blog/BloggingResources

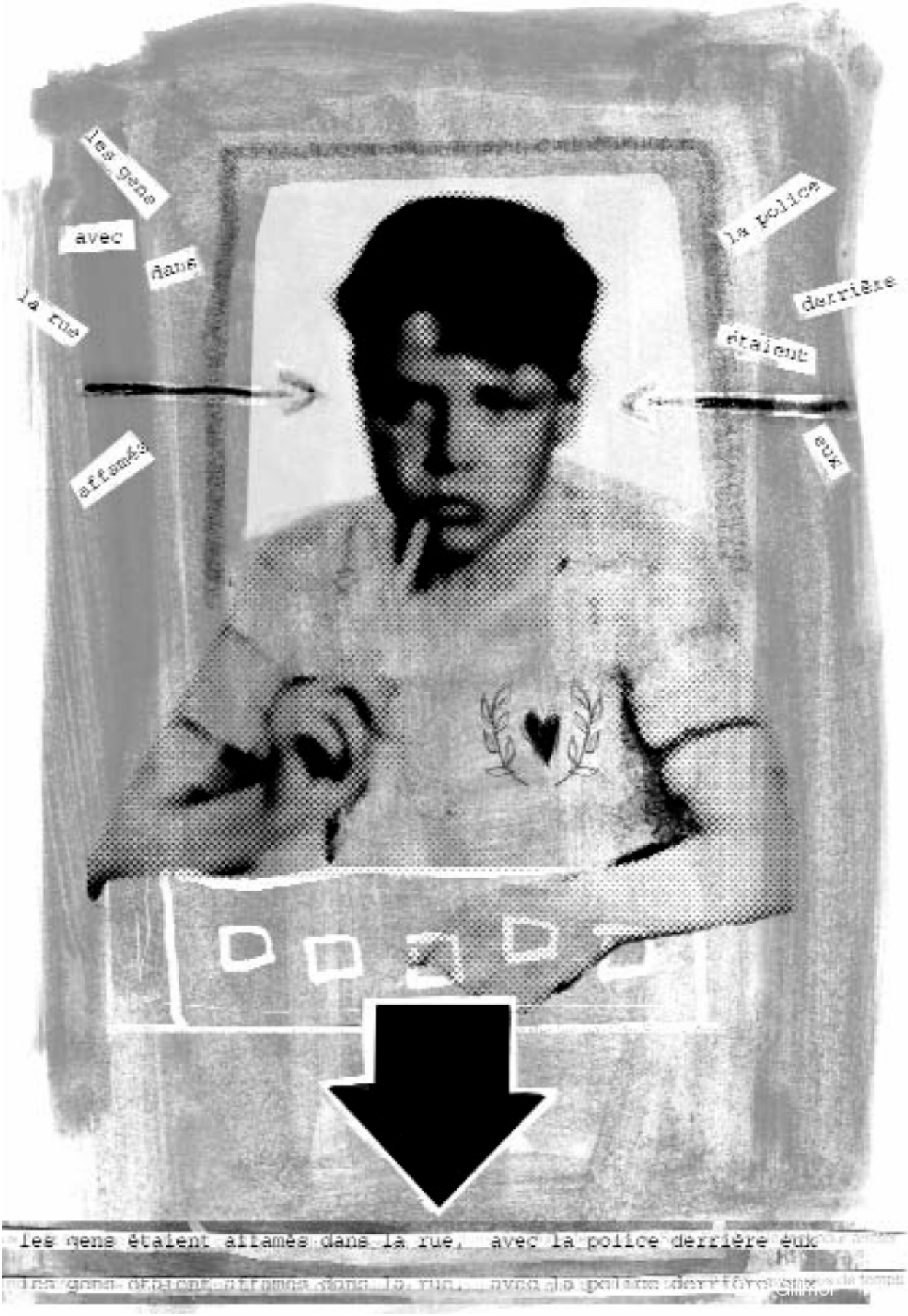
The Weblog Workshop:
http://cyber.law.harvard.edu:8080/globalvoices/wiki/index.php/WeblogWorkshop

How to blog:
http://blogging.typepad.com/how_to_blog

The blogosphere:
http://blog.lib.umn.edu/blogosphere

Blogging 101:
http://www.unc.edu/%7Ezuiker/blogging101/index.html




les gens
avec
dans
la rue
affamés
la police
derrière
étaient
eux
les gens étaient affamés dans la rue, avec la police derrière eux

ЯКОЙ ПАВІННАЯ БЫЦЬ **ЭТЫКА БЛОГЕРА?**

Дэн Гілмар (Dan Gillmor)

Не ўсе блогеры займаюцца журналістыкай. Большасьць зь іх гэтага ня робіць. Але калі ўжо брацца за журналістыку, то неабходна прытрымлівацца пэўных этычных прынцыпаў.
Ці значыць гэта, што блогеры павінныя падпісацца пад нейкім маральным кодэксам? Не абавязкова.

Прафэсійная журналістыка перапоўненая этычнымі кодэксамі. Адныя кодэксы імкнуцца зафіксаваць усе магчымыя парушэньні і таму займаюць болей старонак, чым Канстытуцыя ЗША. Іншыя, кароткія і лаканічныя, даюць рэкамэндацыі, як сябе паводзіць. Кібэр-журналісты адаптавалі для блогераў кодэкс амэрыканскага Саюзу прафэсійных журналістаў і разьмясьцілі яго на сваім сайце (http://www.cyberjournalist.net/news/000215.php). Гэта сур'ёзны і варты высілкаў праект.

Усе этычныя коды ствараюцца з адной важнай мэтай: заваяваць давер. Калі чытач (глядач ці слухач) не давярае тэксту (сюжэту ці паведамленьню), ён ім не будзе цікавіцца. Выключэньнем, безумоўна, зьяўляецца азнаямленьне з неэтычным матэрыялам у навучальных мэтах: назіраючы за неэтычнымі паводзінамі іншых, можна пазьбегнуць шмат якіх памылак.

Для мяне этыка мае дачыненьне да адной вельмі простай рэчы – гонару. Безумоўна, гэта вельмі шырокі панятак. Але, калі чалавек брыдка сябе паводзіць, ён наўрад ці заваюе чыйсьці давер.

У амэрыканскай журналістыцы гонар заўсёды асацыюецца са стандартамі "аб'ектыўнасьці": артыкул павінен прапаноўваць розныя меркаваньні і асьвятляць усе нюансы, каб чытач мог скласьці сваё асабістае меркаваньне. Я лічу, што аб'ектыўнасьць – гэта важная, але недасягальная мэта, таму што кожны з нас укладае свае погляды і пераканьні ва ўсё, што б мы ні рабілі.

У сучаснай журналістыцы, арыентаванай не на лекцыю, але на размову, мараль вызначаецца ня столькі кодэксамі, колькі каштоўнасьцямі і прынцыпамі, што ляжаць у аснове сумленнай журналістыкі.

Асноўныя характарыстыкі добрай журналістыкі: скрупулёзнасьць, дакладнасьць, чэснасьць, празрыстасьць і незалежнасьць.

Межы гэтых прынцыпаў не заўсёды выразныя. Іх можна тлумачыць па-рознаму, у кожным з гэтых словаў безьліч падтэкстаў. Але, на маю думку, гэта правільны шлях да добрай журналістыкі, і кіравацца гэтымі прынцыпамі значна прасьцей у онлайнавай журналістыцы. Давайце разгледзім кожны зь іх паасобку:

СКРУПУЛЁЗНАСЬЦЬ

Калі я быў рэпартэрам, а потым аглядальнікам, я імкнуўся даведацца як мага болей. У рэшце рэшт, факты і меркаваньні – гэта аснова рэпартажа. Болей за ўсё мне падабалася, калі 95 адсоткаў таго, пра што я даведваўся, заставалася па-за межамі артыкула. Найлепшыя зь вядомых мне рэпартэраў заўсёды хочуць зрабіць яшчэ адзін тэлефонны званок, зьвярнуцца да яшчэ адной крыніцы. (Апошняе пытаньне у кожным маім інтэрвію: "З кім яшчэ, на вашу думку, мне было б варта пагутарыць на гэтую тэму?").

Сёньня скрупулёзнасьць – гэта штосьці большае, чым апытаньне людзей, каардынаты якіх ёсьць у нашых запісных кніжках, рэальных ці віртуальных. Гэта, перадусім, зварот да чытачоў. Так я рабіў, калі пісаў кнігу пра народную журналістыку ў 2004 годзе (тое ж самае пачынаюць рабіць і іншыя аўтары ў сваіх кнігах). Нягледзячы на тое, што шматлікія фактары не спрыяюць гэтаму, я ўпэўнены, што ўсё болей і болей журналістаў будуць выкарыстоўваць гэты мэтад.

ДАКЛАДНАСЬЦЬ

Прытрымлівайцеся фактаў.
Кажыце ня толькі тое, што ведаеце, але і папярэдзьце пра пытаньні, адказаў на якія ня ведаеце. Калі чытач (слухач ці глядач) ведае тое, чаго ня ведаеце вы, вы даеце яму (ёй) магчымасьць дапоўніць інфармацыю.
Дакладнасьць значыць неадкладнае выпраўленьне памылак, што нашмат прасьцей зрабіць онлайн, дзе магчыма "зьмякчыць" памылкі, ці хоць бы зьменьшыць шкоду, якую могуць прынесьці новым чытачам нашыя памылкі.

ЗБАЛЯНСАВАНАСЬЦЬ

У адрозьненьне ад дакладнасьці, збалянсаванасьці дасягнуць цяжка. Звычайна збалянсаванасьць – вельмі суб'ектыўная рэч. Але, на маю думку, нават тут можна ўжыць некалькі агульных прынцыпаў.
Збалянсаванасьць, акрамя ўсяго іншага, значыць прыслухоўвацца да розных меркаваньняў і ўключаць іх у журналістыку. Гэта не азначае, што трэба, як папугай, паўтараць усе ілжывыя выказваньні для таго, каб дасягнуць таго "лянівага" балянсу, калі журналісты цытуюць супрацьлеглыя меркаваньні, у той час як факты, відавочна, на карысьць аднаго з бакоў.
Збалянсаванасьць – гэта калі вы даеце магчымасьць выказацца людзям, якія лічаць, што вы ня маеце рацыю, нават калі вы з гэтым ня згодныя. Зноўку ж, гэта нашмат прасьцей зрабіць онлайн, чым у друкаванай публікацыі, ня кажучы пра тэле- ці радыё-перадачы.
І, нарэшце, збалансаванасьць залежыць ад правільнага падыходу. Мы павінныя ўсьведамляць, што намі рухае, і павінныя заўсёды быць гатовыя выслухаць тых, хто з намі не пагпджаецца. Першае правіла пры гутарцы - умець слухаць. Я ўпэўнены, што ад людзей, якія са мной ня згодныя, я навучуся большаму, чым ад тых, хто са мною пагаджаецца.

ПРАЗРЫСТАСЬЦЬ

Паведамленьне пра свае магчымыя канфлікты інтарэсаў робіцца неад'емная часткай журналістыкі. Безумоўна, гэта лягчэй сказаць, чым зрабіць.
Напэўна, ніхто ня будзе спрачацца, што журналісты павінныя асьвятляць такія тэмы, як, напрыклад, канфлікт фінансавых інтарэсаў. Але да якіх межаў? Ці трэба журналістам разгортваць перад усімі сваё жыцьцё, як кніжку? І калі трэба, то наколькі шырока?
Асабістыя перакананьні, нават несьвядомыя, таксама маюць узьдзеяньне на журналістыку. Я - амэрыканец, выхаваны на перакананьнях, якія людзі ў іншых краінах (і нават шмат хто ў ЗША) адкрыта адмаўляюць. Мне трэба быць асьцярожным з рэчамі, якія я ўспрымаю як нешта натуральнае, і час ад часу пераправяраць іх, што я раблю ў сваёй працы таксама.

Наступны шлях да дасягненьня празрыстасьці – праз спосаб прэзэнтацыі рэпартажа. Неабходна як мага часьцей спасылацца на крыніцы, тым самым паказваючы людзям, што вы абапіраецеся на рэальныя факты і дадзеныя.

(Магчыма, гэта тычыцца дакладнасьці і збалянсаванасьці, але й сюды падыходзіць таксама).

НЕЗАЛЕЖНАСЬЦЬ

Адданасьць у журналістыцы – гэта ісьці у сваіх рэпартажах да канца. Гэта немагчыма, калі сродкі масавай інфармацыі аб'яднаныя ў некалькі буйных кампаній, ці танчаць пад дудку ўладаў. Быць незалежным онлайн прасьцей. Можна стварыць блог. Але блогер не

застрахаваны ад ціску з боку рэжыму ці фінансавых складанасьцяў, калі паспрабуе зарабляць сабе на жыцьцё блогінгам.
Выбітны амэрыканскі блогер Джэф Джарвіс (Jeff Jarvis) (buzzmachine.com), дадае яшчэ некалькі каштоўнасьцяў. Блогер павінен паважаць этыку размовы. Ён кажа, што размова вядзе да паразуменьня, што, на маю думку, павінна стаць асноўным прынцыпам гэтага новага сьвету – сьвету блогінгу.
Першае правіла размовы – слухаць. Этыка патрабуе ўменьня слухаць, бо толькі так мы вучымся.

Дэн Гілмар (Dan Gillmor) – заснавальнік Grassroots Media Inc. – кампаніі, якая займаецца разьвіцьём і папулярызацыяй народнай журналістыкі. Першы сайт кампаніі – гэта Bayosphere.com, які асьвятляе падзеі ў наваколькі Сан-Францыска (San Francisco Bay Area). Дэн Гілмар – аўтар кнігі "Мы – мэдыі: народная журналістыка, якую ствараюць людзі для людзей" "We the media: Grassroots Journalism by the People, for the People", выдавецтва "O'Relly Media", 2004 год.

Блог Дэна Гілмара:
http://bayosphere.com/blog/dangillmor

Elisabeth Fall, for O'Reilly Media

ШТО ТРЭБА ЗРАБІЦЬ, КАБ БЛОГ ЗАЎВАЖЫЛІ **ПОШУКАВЫЯ СЫСТЭМЫ**

Аліўе Андрыё (Olivier Andrieu)

Блогі – гэта тыя ж уэб-сайты, таму яны індэксуюцца такімі пошукавымі сыстэмамі, як Google, Yahoo! Search ці MSN Search. Каб блог стаў пасьпяховым, неабходна, каб ён быў прадстаўлены ключавымі словамі на выніковых старонках пошукавых сыстэм. Таму сайт трэба рабіць так, каб ён адпавядаў класыфікацыйным крытэрам, якія выкарыстоўваюцца пошукавымі сыстэмамі.

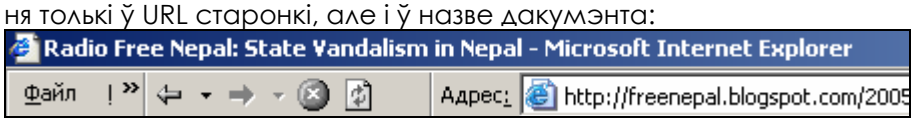
Блогі маюць некалькі ўбудаваных характарыстык, дзякуючы якім пошукавыя сыстэмы іх знаходзяць, індэксуюць і разьмяшчаюць на заўважным месцы на выніковых старонках.

Паколькі блогі – гэта асабістыя дзёньнікі (прынамсі, на пачатку), яны складаюцца пераважна з тэкстаў, дзякуючы чаму пошукавым сыстэмам лягчэй іх знаходзіць. Пошукавыя машыны не заўважаюць сайты, на якіх шмат графікі ці флэш-анімацыі, а тэкставае суправаджэньне мінімальнае.

Кожная "нататка" звычайна займае асобную старонку, даступную праз "пэрмаспасылку" ("permalink") і прысьвячаецца нейкай адной тэме. Пошукавыя машыны "падхопліваюць" такія старонкі часьцей, чым вялікія старонкі з тэкстамі на розныя тэмы (напрыклад, архівы ці хатнія старонкі блогаў).

Загаловак нататкі звычайна ўзгадваецца ў загалоўку старонкі ці ў URL (адрасе). Напрыклад, на блогу Радыё "Свабодны Нэпал" (Radio Free Nepal) http://freenepal.blogspot.com кожная нататка разьмешчаная на асобнай старонцы. Напрыклад: http://freenepal.blogspot.com/2005/04/state-vandalism-in-nepal.html

Загаловак нататкі (State Vandalism in Nepal) (Вандалізм нэпальскіх уладаў) сустракаецца ня толькі ў URL старонкі, але і ў назве дакумэнта:



Radio Free Nepal: State Vandalism in Nepal – Microsoft Internet Explorer

Такім чынам, загаловак нататкі ідзе за назвай блога на хатняй старонцы блога: http://freenepal.blogspot.com

Прысутнасьць апісальных ключавых словаў у загалоўках старонкі (зьмесьціва тэга <TITLE> на мове HTML), а таксама ў URL гэтых дакумэнтаў, зьяўляецца асноўным крытэрам для пошукавых машын. Таму вельмі важна прадумаць загалоўкі нататак, калі вы хочаце, каб іх "падхапілі" пошукавыя машыны.

Тэкставыя спасылкі ўтвараюцца аўтаматычна, перш за ўсё, спасылкі на архівы (гл. прыклады з правага боку на старонках Радыё "Свабодны Нэпал" (Radio Free Nepal).

PREVIOUS POSTS

Peace Bond: Sign of Problems
Must-Read Stories: April 20
Municipal Election: For Covering Up the Death of Democracy
Articles of Interest: April 16
Attempts to Blur Borderlines
Articles of Interest: April 7
Press: Support King or Die
Vote for Radio Free Nepal!
Nepali Congress leader released from house arrest
Articles of Interest: March 30

Гэта вельмі важна для індэксацыі старонак, таму што па тэкставым зьмесьціве спасылак (так званых "якарах" ("anchors") пошукавыя машыны вызначаюць рэлевантнасьць старонак, на якія яны (машыны) даюць спасылкі. Такім чынам, у дадзеным прыкладзе прысутнасьць словаў "Вандалізм нэпальскіх уладаў" ("State Vandalism in Nepal") у першай спасылцы ці "Радыё "Свабодны Нэпал" ("Radio Free Nepal") у дзевятай спасылцы павялічвае рэлевантнасьць старонкі, пазначаную спасылкай дзякуючы гэтым вызначэньням. Да таго ж, старонка з гэтымі спасылкамі (пошукавыя сыстэмы аддаюць перавагу тэкстам, на якія можна "клікнуць"), а таксама старонкі, на якія спасылаюцца, будуць лічыцца рэлевантнымі.

ЯК ЗРАБІЦЬ ТАК, КАБ БЛОГ "ПАДХАПІЛА" ЯК МАГА БОЛЕЙ ПОШУКАВЫХ СЫСТЭМАЎ

У блогаў шмат патэнцыйных магчымасьцяў, якія можна выкарыстоўваць, каб іх "падхапіла" як мага болей пошукавых машын. Як толькі пошукавая машына "заўважае" блог, які або быў "знойдзены" чалавекам ці з дапамогай "павукоў" ("spiders"), якіх пошукавыя машыны пускаюць па спасылках, у блога зьяўляецца значна болей шанцаў, чым у стандартнага ўэб-сайта, патрапіць на першыя пазыцыі (з нагоды ўласьцівых яму перавагаў). Але варта пайсьці далей, каб зрабіць свой блог яшчэ больш заўважным.

Вось некаторыя падказкі, як гэта зрабіць, выкарыстоўваючы асноўныя ключавыя словы, узятыя з канкрэтнай тэмы на вашым блогу:

1. Засяродзьце ўвагу на тэхналёгіі, з дапамогай якой ваш блог "падхопяць" пошукавыя машыны

Калі ваш сайт яшчэ не ў сеціве, вельмі асьцярожна выбірайце тэхналёгію(Bloggers, Dotclear, Blogspirit, Joueb і шмат іншых), з дапамогай якой вы яго там разьмесьціце.
Выберыце тую, у якой болей за ўсё шанцаў на індэксацыю:

- загаловак нататкі павінен быць цалкам прадстаўлены ў загалоўку старонкі (the <TITLE> tag), а таксама ў URL (што робіцца не заўсёды, часам нейкія праграмы "абрываюць" загаловак нататкі пасьля пэўнай колькасьці літар).
- Магчымасьць стварэньня пэрмаспасылак ("permalinks") (спасылак на старонку, на якой разьмешчаная адна нататка)
- Выбраная тэхналёгія павінная забясьпечваць максімальныя магчымасьці для дызайну і пэрсаналізацыі сайта, у прыватнасьці, сваю графіку і пэрсанальную табліцу стыляў (style-sheets). Неабходна авалодаць максімальнай колькасьцю тэхнічных прыёмаў, каб павялічыць магчымасьці сайта на індэксацыю.

Каб праверыць усе вышэйпералічаныя парамэтры, прагледзьце сайты, што выкарыстоўваюць выбраную вамі тэхналёгію (на гэтых сайтах вы знойдзеце дастаткова вялікія ўзоры). Паглядзіце, як выстаўленыя матэрыялы на гэтых сайтах – так вы зможаце шмат чаму навучыцца.

2. Сур'ёзна пастаўцеся да выбару загалоўкаў нататак

Гэта вельмі важна. Загаловак вашай нататкі будзе прадстаўлены ў загалоўках асобных старонак, у URL, а таксама ў тэксьце спасылак, што на іх паказваюць. Гэта тры асноўныя крытэры для пошукавых сістэмаў. Таму назва нататкі павінная ў сьціслай форме зьмяшчаць у сабе найбольш важныя тэрміны. Пазьбягайце загалоўкаў кшталту "Клаясна сказана!", "Вітаю!" ці "Клёва!". У загалоўку нататкі неабходна з дапамогай ня болей чым пяці словаў перадаць зьмест нататкі. Падумайце, ці хочаце вы, каб на тое ці іншае слова ў загалоўку адрэагавалі пошукавыя машыны, і калі слова вас задавальняе, стаўце яго ў загаловак. Спарава, бадай што, нялёгкая, але вельмі плённая.

3. Тэкст

Пошукавыя сыстэмы "любяць" тэксты, вось і дайце іх ім. Можаце выстаўляць колькі заўгодна фотаздымкаў, але абавязкова ў тэкставым суправаджэньні. Пастарайцеся, каб у кожнай нататцы было ня менш за 200 словаў, тады яе хутчэй "падхопяць" пошукавыя сыстэмы. Пошукавікі "ня любяць", калі адна нататка прысьвячаецца некалькім тэмам. Залатое правіла: адна тэма – адна нататка.

4. Зьвяртайце ўвагу на першы абзац нататак

Неабходна збвяртаць увагу і на тое, дзе ў тэксьце стаяць ключавыя словы. З асаблівай адказнасьцю трэба паставіцца да першага абзаца. Калі, напрыклад, вы хочаце, каб вашу нататку можна было знайсьці, напрыклад, на запыт "вызваленьне закладнікаў", пастаўце гэтае словазлучэньне сярод пяцідзесяці першых словаў нататкі. Гэта тычыцца і астатніх ключавых словаў, якія вы выбераце. Пошукавікі хутчэй "падхопяць" старонку, якая пачынаецца з ключавых словаў, чым старонку з ключавымі словамі напрыканцы, нават калі, акрамя гэтага, старонкі нічым болей не адрозьніваюцца. Ключавыя словы можна выдзеліць, напрыклад, тлустым шрыфтам, што сігналізуе пошукавікам, што словы важныя.

5. Пазьбягайце дубляваньня зьместу нататак

Усе пошукавыя сыстэмы ўмеюць вызначаць дубляванае зьмесьціва. Калі дзьве старонкі вельмі падобныя адна да адной, індэксавацца будзе толькі адна зь іх. Другая ж старонка толькі зрэдку патрапляе на старонку з вынікамі пошуку. Google, напрыклад, выдае наступнае паведамленьне: ((Для таго, каб паказаць Вам вынікі, якія найбольш абпавядаюць Вашаму запыту, мы прапусьцілі некаторыя, вельмі падобныя да ўжо паказаных. Вы можаце паўтарыць пошук, дадаўшы прапушчаныя вынікі)).

З блогамі такое здараецца вельмі часта, таму што старонкі з нататкамі выглядаюць вельмі падобнымі.

Напрыклад, калі ў вас аднолькавы ўступ да кожнай старонкі, пастаўце яго ўнізе, альбо вынесіце толькі на хатнюю старонку. Тады вашыя старонкі ня будуць выглядаць падобнымі.

6. Не давайце блогу доўгую назву.

Найлепшая назва (зьмесьціва тэга <TITLE>) для пошукавых сыстэм павінная складацца з 5-10 словаў, без уліку артыкляў, злучнікаў і прыназоўнікаў (так звыных "stop words"). Звычайна загаловак старонкі блога складаецца зь дзьвюх частак:

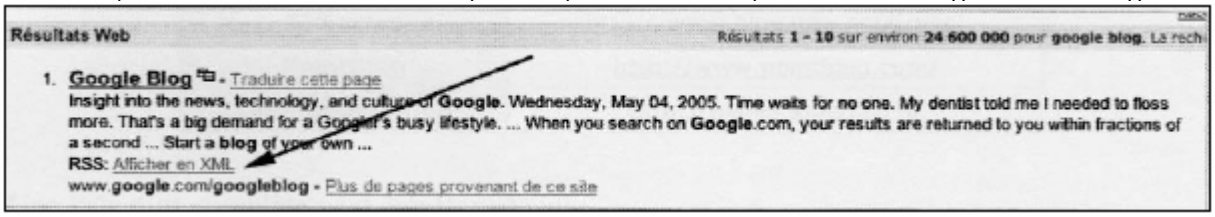
- Агульная назва блога
- Паўтарэньне загалоўка нататкі.

Для таго, каб у галоўным загалоўку старонак, якія прадстаўляюць кожную з нататак, было ня болей за дзесяць словаў, неабходна, каб агульны загаловак блога складаўся з пяці словаў, і загаловак нататкі – таксама з пяці. Гэта няшмат, але сьціласьць і інфарматыўнасьць – гэта адзін з асноўных крытэраў індэксаваньня для пошукавых сыстэм.

Калі гэта магчыма (ня ўсе тэхналёгіі гэта дазваляюць), стаўце спачатку загаловак нататкі, а пад ёю – агульны загаловак блога, а не наадварот.

7. Сындыкуйце свой блог

Большасьць блогавых плятформаў дазваляюць ствараць "XML паток"("XML thread") ці "RSS канал" ("RSS feed"), з дапамогай якіх карыстальнікі маюць доступ да вашых нататак у зручным фартмаце. Вы можаце прапанаваць такую магчымасьць і на сваім блогу (усталяваньне зойме ўсяго некалькі хвілін). Так вы павялічыце колькасьць наведнікаў. Акрамя таго, напрыклад, на Yahoo!, гэта будзе заўважана наступным чынам: ((View as XML))



Так што скарыстайцеся такой магчымасьцю.

8. Рэгулярна абнаўляйце спасылкі

Спасылкі вельмі важныя для пошукавых сыстэм, таму што дазваляюць скласьці рэйтынг папулярнасьці (у Google гэта мае назву PageRank). Каб стварыць спасылкі на свой блог, трэба:

- занесьці яго ў дырэкторыі (гл. ніжэй).
- Заняцца пошукам "сайтаў-сваякоў" ("cousin sites"), якія не зьяўлюцца вашымі канкурэнтамі, але прапануюць матэрыялы на тыя ж тэмы, што і ваш блог. Абмен спасылкамі паміж блогамі ў адной і той жа сфэры інтарэсаў неабходна наладзіць як мага хутчэй (гэта робіцца даволі часта, а таксама ўхваляецца ў супольнасьці блогераў, што зьяўляецца яшчэ адной перавагай блогаў). Блогі таксама прыдатныя для гэтага, таму што палі старонак часта пустыя, і на іх спакойна можна зьмясьціць спасылкі.

ТЭМАТЫЧНЫЯ ДЫРЭКТОРЫІ

Вельмі важна, каб блог індэксаваўся пошукавымі сыстэмамі (такімі, як Google, MSN, Yahoo! ці Exalead), а таксама агульнымі дырэкторыямі (такімі, як Yahoo! Directory і Open Directory). Але індэксацыя па тэмах таксама мае вялікае значэньне, таму што:

- прываблівае наведнікаў, якія сапраўды цікавяцца дадзенай тэмай;
- павялічвае колькасьць спасылак на ваш блог, што спрыяе вашай папулярнасьці;
- робіць вас вядомым іншым блогерам, якія, магчыма, захочуць абменьвацца спасылкамі з сайтамі, падобнымі да іх сайтаў.

Пошукавых інструмэнтаў (пошукавых сыстэмаў і дырэкторыяў), якія індэксуюць блогі, існуе вялікае мноства. Вось некаторыя зь іх:

Англамоўныя	Blogwise:	http://www.blogwise.com/
	Daypop:	http://www.daypop.com/
	Feedster:	http://www.feedster.com/
	Technorati:	http://technorati.com/
	Waypath:	http://www.waypath.com/
	Blogarama:	http://www.bolgarama.com/
	Syndic8:	http://www.syndic8.com/
Франкамоўныя:	Blogonautes:	http://blogonautes.com/
	Blogolist:	http://www.blogolist.com/
	Weblogues:	http://www.weblogues.com/
	Blogarea:	http://www.blogarea.com/
	Pointblog:	http://www.pointblog.com/
	Les Pages Joueb:	http:// pages.joueb.com/

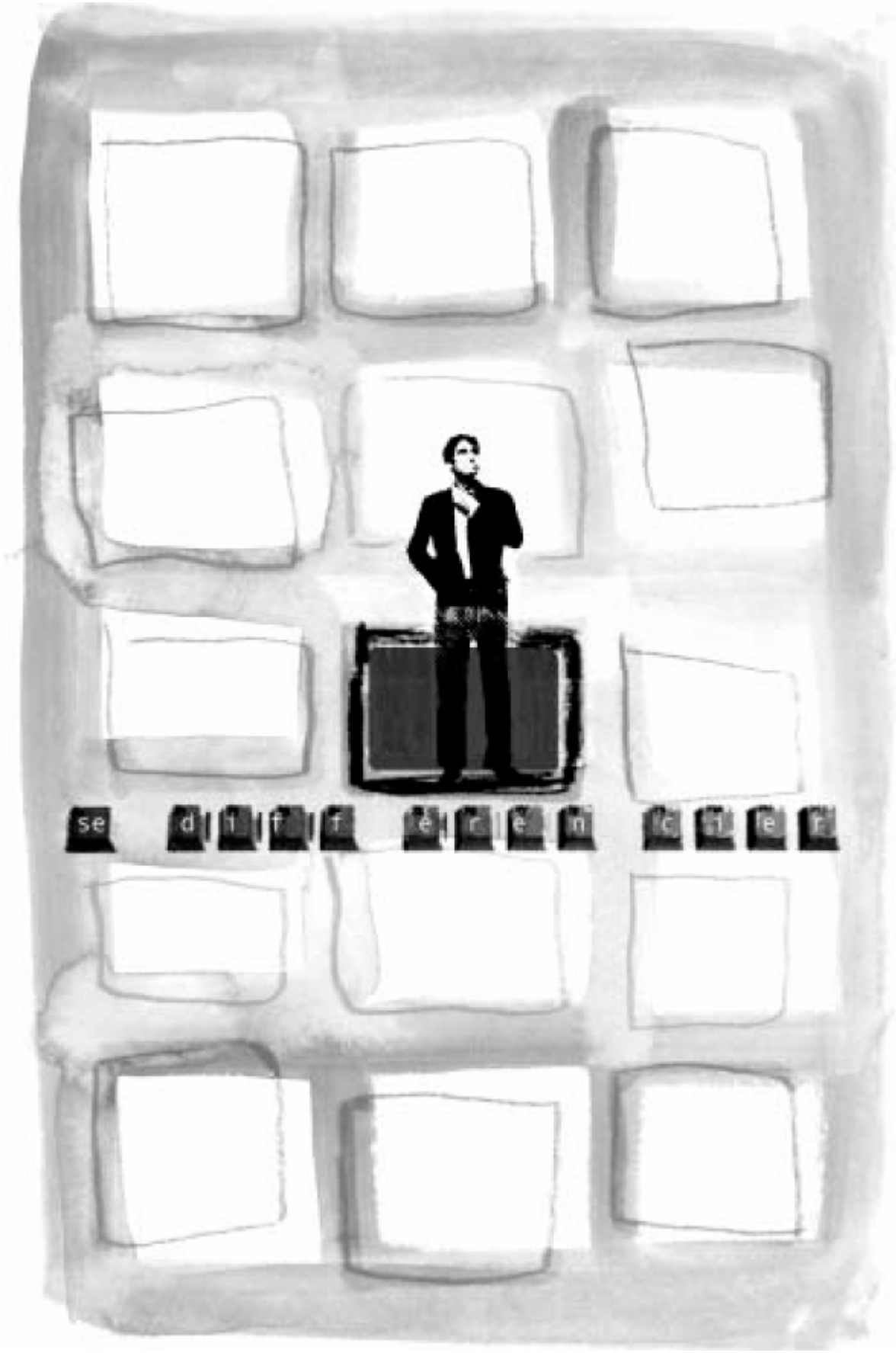
Пашыраны сьпіс можна знайсьці на адрасе:
http://search-engines.blogs.com/mon_weblog/2005/05/les_search-engines_de_.html

Прагледзьце таксама дырэкторыі правайдэраў тэхналёгій:
http://www.canalblog.com/cf/browseBlogs.cfm
http://www.dotclear.net/users.html
http://www.blogspirit.com/fr/communautes_blogspirit.html

ЗАКЛЮЧЭНЬНЕ

Блог мае ўсе парамэтры, неабыходныя для яго індэксацыі пошукавымі сыстэмамі. З дапамогай вышэйпрыведзеных рэкамэндацый вы павінныя атрымаць добрыя вынікі і зрабіць так, каб ваш блог заўважылі. Што ж, у добры шлях! І памятайце, што зьмест – важней за ўсё.

Аліўе Андрыё – незалежны інтэрнэт-кансультант. Ён спэцыялізуецца на праблемах індэксацыі сайтаў пошукавымі сыстэмамі, а таксама вядзе ўэб-сайт: www.abondance.com.


se
d i f f é r e n c i e r

ШТО ЗРАБІЦЬ, **КАБ БЛОГ “ЗАЗЬЗЯЎ”**

Марк Глэйзер (Mark Glaser)

Чым выдзяляецца адзін канкрэтны блог сярод мільярдаў нататак, разьмешчаных на мільярдах блогаў ва ўсім сьвеце? Чым адрозьніваецца ад астатніх блогераў аўтар блога, на які наведнікі вяртаюцца зноў і зноў, і які атрымлівае высокую ацэнку ў сродках масавай інфармацыі?

Справа ў зваротнай сувязі. Посьпеху дасягаюць блогеры, якія падтрымліваюць кантакт са сваімі чытачамі. Незалежна ад колькасьці чытачоў (іх можа быць дзесяць, а можа быць і сто тысяч), блогеры забаўляюць і адукоўваюць іх. Многія імкнуцца падкрэсьліць адрозьненьне паміж блогерамі з аднаго боку і журналістамі, пісьменьнікамі, спэцыялістамі па маркетынгу і ўсімі астатнімі людзьмі, якія пішуць з другога. Але мэта ў іх адна: схапіць чалавека за каўнер і не адпускаць.

Некаторыя з аўтараў гэтай кнігі – Чанад Бахрэйні з Бахрэйна, Ян Шам-Шэклтан з Ганконгу і Араш Сігарчы з Ірана вядуць блогі ў краінах, дзе ўлады ўважліва сочаць за тым, што яны пішуць. Але іх блогі чытаюць ва ўсім сьвеце, каб даведацца пра тое, пра што прэса гэтых краін не адважваецца паведамляць. У краінах, дзе свабода слова і свабода прэсы пад пагрозай, галасы блогераў у сеціве – гэта каштоўная крыніца інфармацыі пра тое, што адбываецца на вуліцах іх гарадоў. Фотаздымкі і паведамленьні на іх блогах – жыцьцёвая неабходнасьць.

Але дзякуючы чаму гэтыя і іншыя вартыя ўвагі блогі “зьзяюць”?
Вось некалькі асноўных характарыстык, якія адрозьніваюць іх ад мільёнаў іншых блогаў:

УНІКАЛЬНАСЬЦЬ

Найлепшыя блогеры маюць свой унікальны голас, адрозьніваюцца сваёй арыгінальнасьцю і расказваюць гісторыі, якія маюць для іх значэньне. У аснове ўэблогаў ляжыць ідэя онлайнавага асабістага дзёньніка. Таму важна памятаць, што весьці дзёньнік – гэта ня тое, што пісаць навуковыя тэксты ці артыкулы для агенцтва навінаў. Чанад Бахрэйні – псэўданім блогера з Азіі. Нататкі на ягоным блогу – гэта ягонае ўспрыняцьце падзей у Бахрэйне - краіне, дзе ён жыве (асноўную частку насельніцтва Бахрэйна складаюць арабы). Ян Шам-Шэклтан – акторка, якая шмат падарожнічала. Яна дапамагала ў арганізацыі акцыі пратэсту супраць блякаваньня блогерскіх сайтаў TypePad кітайскімі ўладамі. Дарэчы, некалькі год таму яна сама дапамагала кітайскім уладам фільтраваць сеціва.

СТАЛА АБНАЎЛЯЙЦЕ СВОЙ БЛОГ

Вельмі сур’ёзная праблема – гэта тое, што большасьць блогаў не абнаўляецца. З той прычыны, што большасьць тых, хто робіць блогі, займаюцца гэтым бясплатна, яны не абнаўляюць свае блогі кожны дзень. Многія пачынаюць блог, разьмяшчаюць некалькі нататак, але ніколі ня маюць часу на яго абнаўленьне. Каб дасягнуць посьпеху, блогерам неабходна рэгулярна пісаць нататкі, быць у курсе тэмаў, якія іх цікавяць, у тым ліку і бягучых падзей. Гэта не азначае, што яны павінныя абнаўляць нататкі дванаццаць разоў на дзень, але наведнікі ня будуць некалькі тыдняў чакаць новай інфармацыі і проста сыдуць.

ПАДТРЫМЛІВАЙЦЕ ЗВАРОТНУЮ СУВЯЗЬ З ЧЫТАЧАМІ І ЗААХВОЧВАЙЦЕ ІХ ДА СУПРАЦОЎНІЦТВА

Адной з характарыстык блога зьяўляецца інтэрактыўнасьць. Існуе шмат спосабаў, як прывабіць чытачоў, заахвоціць іх да дыскусіі і наладзіць зь імі зваротную сувязь. Вы можаце арганізаваць онлайнавае апытаньне, ці даць чытачам свой электронны адрас, альбо проста даць ім магчымасць камэнтаваць нататкі. Джэф Уі атрымаў папярэджаньне ад уладаў Малайзіі за камэнтар аднаго з чытачоў яго блога. Замест таго каб зьняць усе камэнтары са свайго блога, Уі вырашыў "кіраваць" імі, публікуючы толькі камэнтары па тэме тых чытачоў, якія не адмовяцца ад сваіх словаў. Уі таксама пачаў весьці блог на кітайскай мове пад назвай "The Ferryman" ("Паромшчык"). Такім чынам Уі імкнецца ўсталяваць сувязі паміж кітайскай і малайзійскай блогасфэрамі.

КАЖЫЦЕ ПРАЎДУ ЎЛАДАМ

Адныя блогі дазваляюць камэнтаваць нататкі, іншыя складаюцца са старамодных рэпартажаў. Немагчыма сказаць, што так правільна, а так не. Але арыгінальны рэпартаж ці арыгінальны погляд на падзеі зробяць ваш блог не падобным да іншых. На блогу Чанада Бахрэйні можна было пабачыць фотаздымкі і паслухаць аўдыё запісы з акцый пратэсту ў Бахрэйне супраць зьняволеньня грамадзянскага актывіста ў лістападзе 2004 года. Блогер Араш Сігарчы быў арыштаваны і асуджаны на 14 гадоў турэмнага зьняволеньня за тое, што крытыкаваў жорсткі рэжым за арышты іншых журналістаў. Пазьней яго выпусьцілі пасьля таго, як ён заплаціў штраф, але ў ягонай справе была пададзеная апэляцыя. Галоўнае тое, што ўсе гэтыя блогеры , як і многія іншыя, не пабаяліся сказаць праўду ўлада. Яны супрацьстаяць як адзіная блогасфэра ўладам, якія хочуць схаваць праўду.

Марк Глэйзер – аглядальнік "Online Journalism Review" ("Агляд онлайнавай журналістыкі") (www.ojr.org). Гэта выданьне факультэта камунікацый імя Анэнберга Ўнівэрсытэта Паўдзённай Каліфорніі. Марк Глэйзер - пісьменьнік, жыве ў Сан Францыска. Яго электронны адрас: glaze@sprintmail.com

АСАБІСТЫ ВОПЫТ

НЯМЕЧЧЫНА
БАХРЭЙН
ЗША
ГАНКОНГ
ІРАН
НЭПАЛ

НЯМЕЧЧЫНА

“Мы абараняем грамадзянскія правы і правы чалавека”

Маркус Бекедаль (Markus Beckedahl), Netzpolitik.org

Напрыканцы 90-х, ва ўзросьце 20 год, я актыўна падтрымліваў ідэю адкрытага і свабоднага інфармацыйнага грамадзтва. Я і некалькі маіх сяброў заснавалі НДА “Network new media”, галоўная мэта якога - абарона правоў у віртуальнай прасторы. Ужо на працягу пяці гадоў мы абараняем грамадзянскія правы і правы чалавека ў лічбавай сфэры.

Мы арганізуем канфэрэнцыі, удзельнічаем у разнастайных кампаніях, а таксама супрацоўнічаем зь іншымі НДА. Напрыклад, мы кіруем дзейнасьцю “Каардынацыйнай групы грамадзянскай супольнасьці Нямеччыны на Сусьветным саміце па пытаньнях інфармацыйнага грамадзтва (“German Civil Society Coordination Group to the WSIS (World Summit on the Information Society”)).

У першыя гады сваёй палітычнай дзейнасьці я, галоўным чынам, карыстаўся сьпісамі рассылкі. Я разаслаў каля 5000 зводак і паведамленьняў пра сеткавую палітыку. Аднак па гэтых сьпісах я рассылаў інфармацыю невялікаму колу людзей, якое не пашыралася. Блогі ж адкрытыя і празрыстыя. Яны даюць нашмат больш магчымасьцяў “падзяліцца” ведамі, а таксама распавесьці пра сваю працу.

Свой першы блог я распачаў у 2002 годзе, падчас першага этапу WSIS. Я прыехаў у Жэнэву на практыку ад ААН, маючы пры сабе толькі спальнік і ноўтбук. Мне трэба было знайсьці нейкі новы спосаб перасылкі інфармацыі, без выкарыстаньня HTML, бо раней у мяне гэта займала вельмі шмат часу. Я пісаў пра свае ўражаньні ад працы ў ААН у блогу пад назвай “Турпаход у сусьветную палітыку” (“Backpacking to the world politics”). Гэта быў мой першы блог.

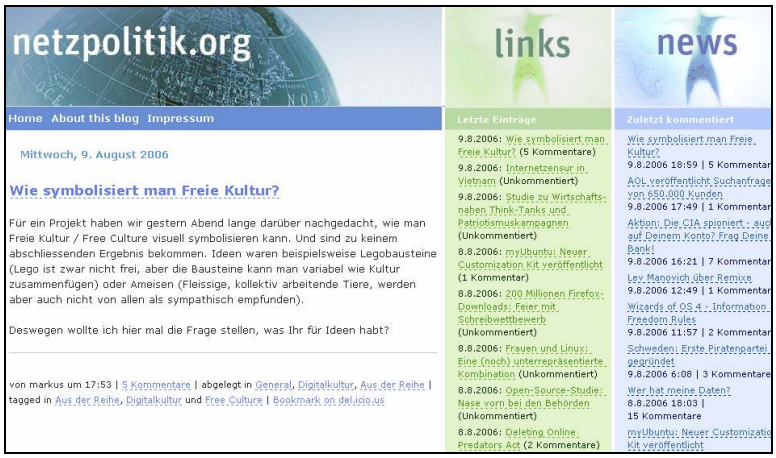
Свой апошні, на дадзены момант, блог netzpolitik.org я распачаў у 2004 годзе. Я выпрабаваў шэраг праграмаў, перш чым спыніў свой выбар на Wordpress – бясплатнай плятформе, якую выкарыстоўвае вялікая супольнасьць. З дапамогай уэблогаў мне вельмі зручна і хутка ствараць, рэдагаваць і публікаваць нататкі.Самае важнае для мяне – гэта інтэрфэйс, які дазваляе сканцэнтравацца на самай важнай працы – напісаньні тэксту, замест таго, каб марнаваць час на разьметку ў HTML. Мне быў патрэбен просты ў выкарыстаньні інтэрфэйс, з дапамогай якога можна сабраць і скампанаваць інфармацыю, набраць тэкст і разьмясьціць яго на сайце, адзін раз націснуўшы на гузік. Усё гэта значна спрасьціла маю працу. Апроч гэтага, мяне яшчэ прываблівае камбінаваная “push-pull” тэхналёгія. Большасьць з маіх чытачоў падпісваецца на RSS канал і чытае мае артыкулы з дапамогай чытальнікаў канала. Астатнія знаходзяць мяне з дапамогай уэб-браўзэраў ці пошукавых сыстэм.

Я зьяўляюся чальцом некалькіх палітычных супольнасьцяў і спрабую зьбіраць усе важныя навіны і разьмяшчаць іх на netzpolitik.org. Гэтыя навіны тычацца грамадзянскіх правоў і правоў чалавека, сьвету як адкрытай крыніцы, магчымасьці свабодна і адкрыта атрымліваць веды, інфармацыйнага грамадзтва для ўсіх, а таксама балянсу ў сфэры аўтарскіх правоў. Свабода слова і свабода самавыражэньня залежаць ад закона аб аўтарскіх правах, а таксама рэгуляваньня лічбавых правоў.
Пагроза грамадзянсім правам існуе ва ўсім сьвеце, у тым ліку і ў Нямеччынне. Новыя меры бясьпекі суправаджаюцца цэнзурай і кантролем. Але пакуль што грамадзтва, часьцей за ўсё, не разумее, што гэта і ёсьць страта свабоды.

Бясплатнае праграмнае забеспячэньне, напрыклад, апэрацыйная сыстэма Linux, прапануе мноства магчымасьцяў для распаўсюджваньня і ўмацаваньня свабоды слова, плюралізму і ўстойлівасьці ў лічбавую эпоху. Безумоўна, я заўсёды карыстаюся Linux. Я

таксама пішу пра навінкі ў бясплатным праграмным забесьпячэньні, пра палітычныя аспэкты выкарыстаньня гэтага праграмнага забесьпячэньня, а таксама тлумачу навічкам, як карыстацца гэтымі сыстэмамі. Я ўважліва сачу за разьвіцьцём онлайнавай энцыкляпэдыі Wikipedia, а таксама за ліцэнзаваньнем creative commons (CC). Зьмесьціва майго блога ліцэнзавана CC, і я актыўна заахвочваю выкарыстаньне і капіраваньне маіх матэрыялаў у некамэрцыйных мэтах, з умовай спасылкі на крыніцу.

Наступная важная тэма – гэта эфэктыўнае выкарыстаньне інтэрнэту – арганізацыямі грамадзянскай супольнасьці, а таксама ў іх кампаніях. Я быў кіраўніком праекту і кансультантам па палітычных камунікацыях у інтэрнэце. Правядзеньню онлайнавых кампаній, а таксама онлайнавай дэмакратыі я прысьвяціў асобную рубрыку ў сваім блогу. Я аналізую магчымасьці выкарыстаньня бясплатных інструмэнтаў для супрацоўніцтва і актыўнай дзейнасьці, а таксама канцэнтруюся на розных аспэктах сацыяльнага праграмнага забеспячэньня, на спосабах, як усім разам у грамадзтве назапашваць як мага больш ведаў.



У netzpolitik.org я таксама зьбіраю інфармацыю і дадзеныя пра будучыя канфэрэнцыі, лекцыі і сустрэчы, прысьвечаныя інфармацыйнаму грамадзтву. Я распавядаю, што адбываецца на канфэрэнцыях, і пішу пра свае ўражаньні ад іх. Кожны дзень я прапаную новы абзор навінаў з мноствам гіпэрспасылак, камэнтую разьвіцьцё новых законаў, а таксама зьвяртаю ўвагу на дзейнасьць НДА ў гэтых рэгіёнах. Мой блог паступова пераўтвараецца ў вузлавую кропку ўнутры нямецкамоўнай грамадзянскай супольнасьці і сетак, адкуль інфармацыя распаўсюджваецца па іншых крыніцах. Я таксама прашу сяброў-блогераў пісаць пра асноўныя праблемы і хутчэй распаўсюджваць навіны. Я выкарыстоўваю RSS чытальнік навінаў (RSS news reader), каб хутка падабраць тэмы для абзору. На працягу першых дзесяці месяцаў мне ўдалося апублікаваць болей за 800 артыкулаў зь мінімальнай дапамогай сяброў.

Я вельмі зьдзівіўся, калі даведаўся, што мой блог штодзень чытае 2500 чалавек. Мне шмат пішуць, асабліва моладзь, якой я раю распачынаць свае ўласныя блогі.

На шчасьце, у Нямеччыне дзейнічаюць законы, якія абараняюць свабоду слова. Мяне не пасадзяць у турму за крытыку ўрада. Я захапляюся адвагай тых людзей, што жывуць ва ўмовах дыктатуры, і рызыкуюць сваімі жыцьцямі, абнаўляючы блогі.

Маркусу Бекедалю 28 гадоў. Ён - выканаўчы кіраўнік newthinking communications – агенцтва, якое займаецца тэхналёгіямі і стратэгіямі адкрытых крыніц інфармацыі. Ён таксама зьяўляецца су-заснавальнікам і старшынём нямецкай НДА, якая займаецца аховай лічбавых правоў "Netzwerk Neue Medien". Яго блог: www.netzpolitik.org.

БАХРЭЙН

“Мы зьнішчылі дзяржаўную манаполію на навіны”

Чанад Бахрэйні (Chan’ad Bahraini)

Для таго, каб распачаць свой блог, я меў дзьве нагоды: 1) пісаць без фармальных абмежаваньняў, тэрмінаў ці патрабаваньняў і 2) паспрабаваць зрабіць свой унёсак у абмеркаваньне праблем, што існуюць у Бахрэйне, а таксама заахвоціць іншых да абмеркаваньня праблем, якія асноўныя сродкі масавай інфармацыі вельмі рэдка асьвятляюць належным чынам.

Сёньня ўсе тэле- і радыё-станцыі, што існуюць у Бахрэйне, падпарадкоўваюцца ўладам, такім чынам, няма рэпартажаў, якія б мелі хоць бы аддаленае дачыненьне да мясцовай палітычнай сытуацыі. Усе мясцовыя газэты прыватныя, такім чынам, яны маюць трохі болей свабоды, чым тэлебачаньне і радыё. Але нават у друкаванай прэсе сытуацыя не нашмат лепшая, таму што рэдактары не адважваюцца адкрыта крытыкаваць асобных уплывовых асобаў, напрыклад, тых, хто ва ўрадзе ці каралеўскую сям’ю (асабліва караля і яго дзядзьку - прэм’ер-міністра).

Аднак інтэрнэт дае магчымасьць свабодна і адкрыта казаць сваё меркаваньне, без кантролю з боку ўладаў. Хоць урад Бахрэйна і мае вопыт нагляду за палітычнымі ўэб-сайтамі і іх блякаваньня, за апошнія год-два ён (урад), здаецца, крыху аслабіў кантроль, але, у той жа час, сытуацыя пагоршылася. Тым ня менш, лёгкасьць, зь якой чалавек можа распачаць уэб-сайт і ананімна пісаць (так, як раблю я), стварае цяжкасьці для ўладаў, якія спрабуюць з гэтым змагацца.

Я хацеў мець магчымасьць свабодна і адкрыта абмяркоўваць розныя тэмы (у тым ліку і палітыку), асабліва ў сітуацыі, калі краіна спрабуе перайсьці да дэмакратыі. Натуральна, я выбраў інтэрнэт, каб дзяліцца зь іншымі людзьмі сваімі думкамі і меркаваньнямі. Мяне падбадзёрваў і той факт, што піянэр блогерскага руху ў Бахрэйне Махмуд (www.mahmood.tv) на той момант, калі я распачаў блог, ужо год вёў свой блог без канфліктаў з уладамі.

Адна з галоўных мэтаў майго блога – гэта абмеркаваньне і аналіз падзеяў у Бахрэйне. Але з прычыны абмежаванага доступу да інфармацыі зь першых крыніц я сам спрабую займацца псэўда-журналістыкай. Гэта значыць, што, калі ёсьць такая магчымасьць, я стараюся прымаць удзел у розных акцыях (асабліва ў дэманстрацыях пратэсту), а потым пішу пра гэтыя падзеі ў сваім блогу, а таксама разьмяшчаю фотаздымкі з гэтых акцый.

Цяпер у Бахрэйне некалькі блогераў, і іх дзейнасьць мае станоўчыя вынікі. Створаная прастора, дзе можна адкрыта абмяркоўваць вялікае мноства тэмаў. Пра сябе магу сказаць, што я знайшоў на іншых блогах Бахрэйна шмат такой інфармацыі, якую б ня змог атрымаць ніколі і ніадкуль. Гэтая супольнасьць існуе ня толькі онлайн - шмат блогераў Бахрэйна сустракаюцца раз на месяц, каб абмеркаваць тыя тэмы, якія мы абмяркоўваем у сваіх блогах.

Аднак онлайнавая дзейнасьць у Бахрэйне больш актыўная на шматлікіх арабскамоўных дыскусійных форумах, якія зьявіліся нашмат раней (напрыклад, bahrainonline.org). Блогінг яшчэ ня стаў шырока распаўсюджанай зьявай у Бахрэйне, аднак нашыя сайты чым далей, тым болей успрымаюцца як “блогі-масты” (“bridge blogs”) (гэты тэрмін увёў Хусэйн Дэракшан (Hossein Derakshan: http://hoder.com/weblog/archives/013982.shtml).
Паколькі большасьць блогераў у Бахрэйне піша на ангельскай мове, мы можам кантактаваць зь людзьмі ва ўсім сьвеце. Для іх мы – крыніца інфармацыі пра тое, што “насамрэч” адбываецца ў Бахрэйне.

Напрыклад, калі ў лютым 2005 года былі арыштаваныя тры мадэратары Bahrainonline.org, мы напісалі пра гэта ў сваіх блогах. Такім чынам, гэтая навіна разьнеслася па сьвеце хутчэй, чым пра яе даведаліся ў Бахрэйне. Ужо ў дзень арышту "Рэпартэры бязь межаў" зрабілі заяву пра гэта. Мне здаецца, што ўвага міжнароднай грамадзкасьці, што была прыцягнутая да гэтых падзеяў, паспрыяла таму, што празь некалькі тыдняў улады вырашылі выпусьціць траіх арыштаваных. Калі гаварыць больш агульна, то нашыя блогі зьнішчылі манаполію дзяржавы на паведамленьне навінаў пра Бахрэйн зьнешняму сьвету.

У прынцыпе, блогеры ў Бахрэйне не перасьледаваліся ўладамі за тое, што пішуць у сваіх блогах. Аднак з пачатку гэтага года сытуацыя пачала зьмяняцца. Як я ўжо казаў, у лютым былі арыштаваныя трое мадэратараў онлайнавага дыскусійнага форуму за тое, што іх нататкі нібыта "распальвалі нянавісьць да ўрада". Адзін з траіх мадэратараў, Алі Абдулеман (Ali Abdulemam), яшчэ і вёў свой блог.
Далей, у красавіку ўрад заявіў, што цяпер усе, хто мае свае ўэб-сайты, павінныя рэгістравацца ў Міністэрстве інфармацыі, інакш іх чакае перасьлед у адпаведнасьці з заканадаўствам. Гэта сьведчыць пра тое, што ўлады ўсё яшчэ да канца не разумеюць, што такое інтэрнэт (а таксама блогі), і ня ведаюць, як справіцца з сытуацыяй, адчуваючы, што ім пагражае небясьпека з боку тых, хто піша онлайн.

Чанад Бахрэйні – выхадзец з паўднёва-ўсходняй Азіі. Зараз жыве ў Бахрэйне, дзе вядзе свой блог http://chanad.weblog.us. Ён вырашыў захоўваць ананімнасьць.

ЗША

“Цяпер я магу пісаць тое, што думаю”

Джэй Роузэн (Jay Rosen), PressThink

Калі я пачаў цікавіцца, як зрабіць уэблог, я атрымаў шмат розных адказаў. Але адну параду давалі ўсе: ты павінен пісаць кароткія нататкі. “Такі стыль”, казалі адныя. “Менавіта гэта працуе”, казалі іншыя. І, нарэшце, найбольшы недавер у мяне выклікаў адказ: “Гэта менавіта тое, што патрэбна занятым чытачам, што працуюць у сеціве. У іх няма часу на твае доўгія і сур’ёзныя аналітычныя артыкулы”. Так казалі ўсе.

Гэта выклікала ў мяне падазрэньні. Я не зьбіраўся пісаць доўгія нататкі па 2000 словаў кожную; але менавіта так і атрымалася, калі я паспрабаваў выкласьці свае думкі ў нататках так, каб сказаць штосьці, чаго не казалі іншыя, і каб гэтыя нататкі былі заўважаныя. (Я магу пісаць сьцісла, калі захачу). Я вырашыў не абмяжоўваць сябе: самому высьветліць, што працуе, а што не, і якім хоча быць PressThink.

Разважаньні кшталту “У людзей няма часу на...” мяне не пераканалі, я не давяраў ім. Такія парады абмежавалі б маю свабоду пісаць тое, што я думаю. Я распачынаў PressThink з мэтай вызваліцца: “Ўаў! Цяпер я маю свой уласны часопіс. Цяпер я магу пісаць тое, што думаю.” Мяне цікавілі карыстальнікі, якія мелі час, каб спусьціцца на глыбіню, ці акеану, ці нататкі, і неістотна, колькі іх будзе.

У мяне быў наступны падыход: гэта мой часопіс, PressThink... Калі ён вам спадабаўся, вяртайцеся. У абстрактным сэнсе, магчыма, мой блог зьяўляецца часткай рынку, ён змагаецца за чытачоў з шоў гульняў, футболам і паўторамі перадачы “Закон і парадак” (“Law and Order”). Але гэта не зусім так. PressThink – вольны грамадзянін у дзяржаве добраахвотнікаў, яму ня трэба паводзіць сябе як які рынкавая адзінка. Такім чынам, мой экспэрымэнт – гэта даўгі блогінг.

Неабходна памятаць, што сеціва прыдатнае для шмат якіх супрацьлеглых рэчаў: каб знайсьці дакладную інфармацыю ці павярхоўна прабегчыся па тэме, каб проста паразмаўляць ці наладзіць сумесную дзейнасьць. Сеціва таксама зазірае ў глыбіні, запамінае інфармацыю, гэта і імгненная бібіліятэка, і фільтр. Меркаваньне не выкарыстоўваць уэблог для пашыранага аналізу, таму што большасьць карыстальнікаў ня стане ў гэта паглыбляцца, падыходзіць для мэдый, а не для сеціва. Але я не працую ў мэдыях! Дзіўная рэч – я намагаюся пісаць сьцісла, але ў выніку атрымліваюцца доўгія артыкулы. Некаторыя чытачы робяць заўвагі: “Занадта шмат словаў не па тэме!” – тыповая выява незадаволенасьці, але зь цягам часу такія заўвагі пачалі мяне забаўляць.

Кожны добры блог засылае ў сеціва пытаньне: ці ёсьць тут попыт на нешта арыгінальнае... на мяне? Але для таго, каб высьветліць, у чым палягае арыгінальнасьць, неабходна мець нейкі вопыт блогінгу.

Назва майго блогу “PressThink” (“Мысьленьне прэсы”) паходзіць ад такіх паняткаў, як, напрыклад, “group think” (“мысьленьне групы”), толькі ў мяне група – гэта прэса. Мая назва – гэта яшчэ і скарачэньне ад “press thinking” (“мысьленьне прэсы”) – дактрыны, ці філязофіі, па якой жывуць журналісты – можна нават сказаць, рэлігіі прэсы. Гэта тое, што мяне цікавіць. “Press think” (“Мысьленьне прэсы”) – гэта тое, чым я сам кіруюся, як крытык і пісьменьнік, а таксама як блогер.

Мая мэта – вычленіць гэты фэномэн - “філязофія прэсы” (“press think part”) з сучасных падзеяў, якія тычацца прэсы, а потым дасьледаваць яго, або прыцягнуць іншых да гэтага дасьледаваньня. Вось што значыць мая назва. Мой блог – “пра” “мысьленьне прэсы” (“press think”); гэта яшчэ і мэханізм,празь які я спрабую прымусіць прэсу мысьліць больш. На маю думку, некаторыя блогеры не прадумваюць належным чынам назвы сваіх блогаў. Я ж, у сваю чаргу, не распачынаў блог, пакуль не выбраў спраўную назву.

Я пакідаю ідэалягічна афарбаваную крытыку прэсы іншым асобам ці арганізацыям, якія з радасьцю гэтым займаюцца, і ў іх гэта добра атрымліваецца. “PressThink” – гэта сайт, які не адсочвае, наколькі аб’ектыўныя мэдыі, хоць я і пісаў пра тых, хто гэтым займаецца. “PressThink” не гоніцца за сэнсацыямі, але я таксама пісаў і пра тых, хто гэта робіць. Я не падтрымліваю Джорджа Буша, але я пішу пра філязофію яго прэсы. Ва ўступе да свайго ўэблогу я напісаў: “Я спрабую выявіць, якія наступствы мае ў сьвеце тое, што мы маем такую прэсу, якую маем.

Неяк мяне запыталі, ці маю я нейкі “мэтад” блогінгу. Я чытаю прэсу, гляджу навіны, праходжуся па сваім сьпісе спасылак (“blogroll”), і такім чынам палюю на нешта апэтытнае, актуальнае і цікавае. Потым я зьбіраю спасылкі і пачынаю пісаць. Альбо нехта дасылае мне па электроннай пошце нешта, на падставе чаго я пішу нататкі. Нярэдка адбываецца нейкая падзея, і я ведаю, што мае чытачы захочуць даведацца, што я пра гэта думаю, і я пішу нататку. Замест нейкага цьвёрдага мэтада я маю нешта накшталт рэкамэндацый па стылі – гэта інструкцыі, як весьці мой блог PressThink, якія я напісаў сам для сябе.

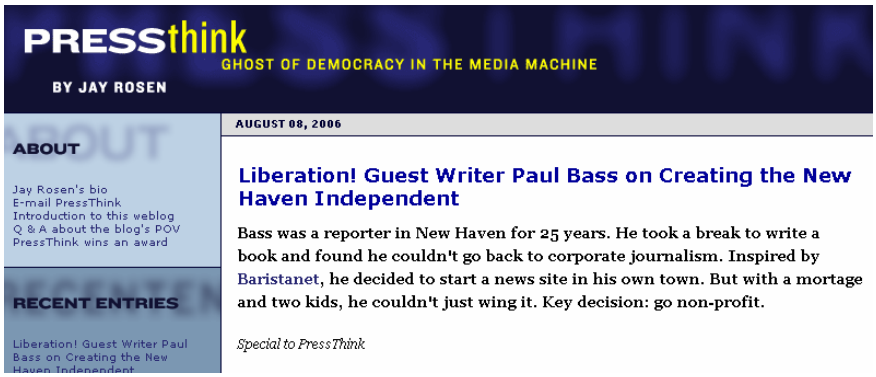
У тыповай нататцы майго блогу, як, напрыклад у гэтай: “Спакойна адкласьці газэту і забыцца на яе” (“Laying the Newspaper Gently Down to Die”) http://journalism.nyu.edu/pubzone/weblogs/pressthink/2005/03/29/nwsp_dwn.html ёсьць пяць асноўных элемэнтаў: загаловак, падзагаловак, эсэ, дапаўненьні (заўвагі і спасылкі), а таксама камэнтары. Кожная з гэтых частак патрабуе свайго стылю. Загаловак у сьціслай форме перадае зьмест нататкі і прыцягвае ўвагу. Падзагаловак тлумачыць праблему і зьмяшчае абзор эсэ. Эсэ – гэта эсэ. Звычайна гэта 1500-2500 словаў, але з 20 ці 30 спасылкамі, якія самі на сябе паказваюць. У дапаўненьнях нататка рэдагуецца. Тут таксама можна назіраць пашыраныя дыскусіі ў благасфэры, у тым ліку і рэакцыю на мае нататкі. З камэнтароў пачынаецца дыялог.

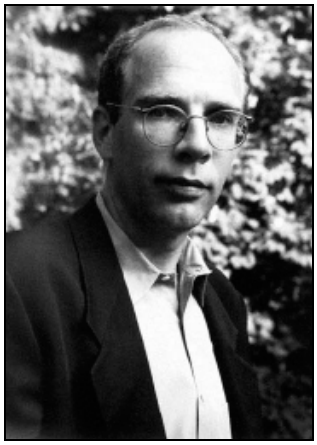
Пасьпяховай я лічу такую нататку свайго блогу, калі гэтыя пяць частак не супярэчаць адна адной. Я лічу, што праца над нататкай не закончаная, пакуль да яе няма дапаўненьняў, зваротных спасылак і камэнтароў. Часам на гэта ідзе болей за тыдзень. Гэта адзін з этапаў вядзеньня блогу. Калі нататка “працуе” (што немагчыма прадбачыць), то ў нейкі момант яна пераўтвараецца ў форум па тэме, якую закранае, і вось гэты форум – гэта тое, што “думае”. Безумоўна, я выпрацаваў свае рэкамэндацыі па стылі, а таксама логіку разьмяшчэньня нататак у адпаведнасьці з гэтымі рэкамэндацыямі, выключна мэтадам спробаў і памылак. Вось чаму толькі пасьля нейкага вопыту вядзеньня блога можна зразумець, што патрэбна, каб рабіць гэта добра.

Пакуль я не распачаў PressThink, мне даводзілася праводзіць усе мае ідэі наконт журналістыкі і журналістаў праз “галкіпераў” ад прэсы, пра якіх я пісаў. Але цяпер, калі я

маю сваё ўласнае выданьне, мне ўжо ня трэба гэтага рабіць. Тыя “галкіперы” самі прыходзяць на мой блог, каб прачытаць, што я думаю. Гэта вялікая розьніца. Нарэшце я маю інтэлектуальную свабоду.

Джэй Роўзэн (Jay Rosen) жыве ў Нью-Ёрку і выкладае журналістыку ўва Ўнівэрсытэце Нью-Ёрку. На факультэце журналістыкі ён працуе з 1986 году, з 1999 па 2005 узначальваў катэдру журналістыкі. Роўзэн – аўтар PressThink - блога пра журналістыку і яе суровыя выпрабаваньні (www.pressthink.org). Гэты блог ён распачаў у верасьні 2003 году: http://journalism.nyu.edu/pubzone/weblogs/pressthink





ГАНКОНГ

“Я стрымала абяцаньне, дадзенае тым, хто загінуў”

Ян Шам-Шэклтан (Yan Sham-Shackleton)

3 араз 12:23, ноч на 4 чэрвеня. Сёньня – 16-я гадавіна масавага расстрэлу на плошчы Цяньаньмынь у Пэкіне. У гэты дзень у 1989 годзе разам зь іншымі галадоўшчыкамі я сядзела ў тунэлі побач з офісам інфармацыйнага агенцтва “Сіньхуа” ў Ганконгу. Гэта была забастоўка ў знак салідарнасьці з кітайскімі студэнтамі. Мы хацелі дэмакратыі для іх і для сябе.
Мы болей не хацелі быць каляніяльнымі падданымі Брытаніі, і не хацелі падпарадкоўвацца камуністычнай партыі. Мы хацелі быць вольнымі.

Празь дзьве-тры гадзіны я пачула па радыё першыя стрэлы, пад гукі сьпеваў, крыкаў і гудзеньне танкаў, ад якога вібравалі сьцены. Мы паглядзелі адзін на аднаго і пабачылі сьлёзы ў вачах.

Цяпер мы ўсе ведаем, што Кітай выкарыстоўвае танкі супраць змагароў за дэмакратыю, але да таго моманту мы пра гэта ня ведалі. Напэўна, у той самы момант, калі я сядзела ў тунэлі, асьветленым яркім флуарэсцэнтным сьвятлом, і чула, як гіне Дэмакратычны рух 1989 году, і нарадзілася ідэя стварыць “Glutter”. Мне было 15 год.

Нават калі і ня ў той момант, то хутка пасьля таго. Я дала абяцаньне, якое магла даць толькі маладая дзяўчына без жыцьцёвага вопыту. Я ні на кроплю не сумнявалася, што выканаю сваё абяцаньне:
“Я ніколі не забудуся пра гэта. Абяцаю, што буду памятаць гэта вечна. Я пражыву сваё жыцьцё лепей дзеля ўсіх вас, таму што я жыву, а вы ўжо не. Я не дапушчу, каб гэта паўтарылася. Я буду нагадваць сьвету пра вас, студэнтаў з плошчы Цяньаньмынь. Мае героі. Мае старэйшыя браты і сёстры”.

Я давала гэтыя наіўныя абяцаньні, сьпяшаючыся і баючыся. Я ня думала пра тое, як штосьці накшталт гэтага можна выканаць, і ці магчыма гэта ўвогуле. Я толькі ведала, што гэта гучыць правільна, ды й дарослыя крычалі тое ж самае з рэпрадуктараў.

Толькі сёньня я ўсьвядоміла, што ўсе мае нататкі, усе фотаздымкі і мастацкія творы, усё, што я рабіла ў імя дэмакратыі, кібэр-пратэсты, якія я арганізоўвала, інтэрвію, якія давала і аповеды, якія публікавала ў імя свабоды слова, - усё гэта я рабіла ня толькі таму, што палымяна ў гэта верыла, але і таму, што гэта быў спосаб супакоіць маю падсьвядомасьць. З дапамогай блогінгу я выконваю абяцаньне, якое дала загінулым.

Я пішу пра гэта, таму што хачу, каб людзі ведалі, чаму я стварыла “Glutter” – не таму, што кіравалася нейкімі правіламі ці кагосьці імітавала. Не таму, што мне хацелася ўвагі ці славы. Мне болей даспадобы, калі на блогу зацішак. Час ад часу я раблю невялікую паўзу, калі адчуваю, што ён прыцягвае занадта шмат увагі, таму што толькі ў стане спакою і бязь ціску я магу пісаць тое, што хачу, і распавядаю пра тое, пра што трэба распавесьці.

Тым, хто хоча распачаць свой блог, я б параіла наступнае: ня слухайце нікога, акрамя саміх сябе. Не чытайце чужыя блогі і не спрабуйце імітаваць іх. Не сядайце са сьпісам "таго, што неабходна рабіць" і не спрабуйце гэта выканаць. Я парушыла безьліч правілаў, таму што ня ведала пра іх існаваньне, і ў мяне атрымалася.

Усё, што вам трэба, каб распачаць блог, - гэта жаданьне яго распачаць.

Усё, што вам трэба, каб яго весьці, - гэта жаданьне пісаць пра тое, пра што вы хочаце распавесьці.

У кожнага з нас быў у жыцьці момант палітычнага прабуджэньня - гэта спускавы мэханізм, які прымусіў нас убачыць несправядлівасьць, з якой трэба змагацца. Інакш ніхто б з нас не пачаў дзейнічаць, не хацеў бы нешта ствараць. Няхай усьведамленьне гэтага кіруе вамі. Спадзяюся, што вам удасца "запаліць" іншых сваімі пераканьнямі і натхніць на барацьбу за зьмены. Вось і ўся "мудрасьць", якой я магу сёньня падзяліцца.

Зараз 2:33 ночы. Я чую кулямётныя чэргі. Тра-та-та-та. Я чую іх з году ў год у гэты час. Мне было 15. Напэўна, я была занадта маладая для такога вопыту. Але яны былі занадта маладыя, каб паміраць.

Ян Шам-Шэклтан хоча, каб вы ведалі, што за шэсьць тыдняў яна напісала шэсьць варыянтаў гэтага артыкула. Яна спрабавала напісаць пра тое, што яна ведае пра блогінг, пакуль не зразумела, што трэба быць самой сабой.

У сваім блогу glutter.com яна распавядае пра мастацтва і палітыку. Блог, у якім аўтарка піша адкрыта і сьцьвярджае сваю пазыцыю ў падтрымку сапраўднай дэмакратыі ў Ганконгу, стала цэнзуруецца ў Кітаі.

ІРАН

“У блогах мы можам пісаць свабодна”

Араш Сігарчы (Arash Sigarchi)

Сёньня мы разумеем выказваньне Маршала Маклюэна: “Сьвет – гэта глабальная вёска” лепей, чым калісьці ён сам. Нябачныя ніткі сеціва даносяць да нас інфармацыю пра тое, што адбываецца ў Азіі, паўдзённай і паўночнай Амэрыках, Эўропе ці на далёкім востраве ля берагоў Афрыкі.
На працягу многіх гадоў журналістыка сутыкаецца з абмежаваньнямі, але цяпер гэтыя абмежаваньні можна пераадолець з дапамогай новых тэхналёгій.

Я – журналіст у краіне, дзе абмежаваньні не даюць мне выконваць маю працу. Акрамя “арганізацыйных” фактараў, якія існуюць у большасьці мэдыяў сьвету, існуюць яшчэ і “зьнешнія” фактары, такія, як заканадаўчыя абмежаваньні, уплыў урада ці нейкіх асобаў, аднабаковая падтрымка сродкаў масавай інфармацыі і г.д. Групы ціску і ўладальнікі капіталу ў маёй краіне маюць большы ўплыў, чым у больш разьвітых краінах. Такім чынам, я вымушаны думаць пра незалежнасьць маёй краіны, пра праўдзівыя навіны пра маю краіну і пра мой аналіз навінаў. У якасьці аднаго са спосабаў пераадоленьня бар’ераў я выбраў блогінг.

У блогах мы можам пісаць свабодна. Разьмясьціць навіны ці нататкі ў блогу нашмат хутчэй, чым друкаваць іх ці агучваць на тэлебачаньні ці радыё. Блогі можна разглядаць, як маленькія інфармацыйныя ці аналітычныя агенцтвы, дзе аўтар адначасова зьяўляецца і карэспандэнтам, і галоўным рэдактарам.

Нехта кажа, што ў блогах трэба разьмяшчаць меней навінаў. Людзям даспадобы распавядаць у блогах пра сваё паўсядзённае жыцьцё. У такіх пісьменьнікаў-аматараў меней чытачоў, звычайна гэта толькі сябры і сваякі.

Але блогі вядомых журналістаў, дзеячаў мастацтва, палітыкаў, эканамістаў, грамадзкіх дзеячаў і спартоўцаў, нават калі яны пішуць толькі пра сваё паўсядзённае жыццё, прыцягваюць увагу, таму што гэта навіны з жыцьця вядомых асобаў. Гэтыя людзі могуць пісаць на мноства тэмаў і прыцягваць увагу чытачоў.

На маю думку, кожны блог прыцягвае ўвагу сваіх чытачоў, у залежнасьці ад іх інтарэсаў. Такім чынам, у адносінах да вядзеньня блогаў не можа быць ніякіх абмежаваньняў.

Я выбраў два спосабы вядзеньня блога. Першы: я неафіцыйна (па-простаму) пішу пра сваё стаўленьне да сучасных падзеяў. Другі спосаб: я разьмяшчаю навіны, аналітыку, інтэрвію, рэпартажы ці эсэ. Такім чынам, я ахоплівaю абедзьве групы чытачоў: першая – гэта тыя, хто хоча даведацца, чым я цяпер займаюся, другая – тыя, хто хоча даведацца пра мае меркаваньні, як журналіста, пісьменьніка і паэта.

Блог, як онлайнавы сродак масавай інфармацыі, дае яго аўтару магчымасьць знаёміцца з адкрытымі меркаваньнямі і крытыкай чытачоў, а таксама разьвівацца. Шчыльны кантакт з чытачамі дае блогеру магчымасьць наўпрост зьвяртацца да чытачоў, а таксама пісаць пра тое, што чытачам даспадобы.

Як я ўжо пісаў, калі вы хочаце надрукаваць кнігу, верш, апавяданьне ці нават газэту або часопіс у Іране, трэба лічыцца з цэнзурай. Такім чынам, многія іранскія пісьменьнікі вядуць блогі – гэта і таньней, і іх ніхто не прымушае правіць тэксты. Але ўлады, як у Кітаі і іншых краінах, абмяжоўваюць карыстаньне інтэрнэтам.

З дапамогай інтэрнэт-журналістыкі можна дабіцца большай свабоды слова і плюралізму меркаваньняў. Нягледзячы на тое, што іранскі суд вынес мне прысуд, я не губляю надзеі. Я ўпэўнены, што ў бліжэйшыя гады тыя, хто кіруе маёй краінай, будуць вымушаныя паважаць як права на свабодны доступ да інфармацыі, так і свабоду слова.

Журналіст і блогер Араш Сігарчы нарадзіўся ў 1978 годзе, падчас рэвалюцыі, якая скінула шаха. Журналістыкай пачаў займацца ў 1993 годзе, калі яму было ўсяго 15 год. Пасьля таго, як у 1997 на пост прэзыдэнта быў абраны прыхільнік рэформаў Мохамад Хатамі, Сігарчы пачаў працу ў выданьнях, якія падтрымлівалі рэформы. Пасьля таго, як у красавіку 2000 году выданьне, дзе ён працаваў, было зачыненае, ён пасяліўся на поўначы Ірана, дзе рэдагаваў газэту "Gillan Emrouz" (цяпер "Gillan"), якая выходзіла кожны дзень на дванаццаці старонках.

Займацца блогінгам Араш Сігарчы пачаў у 2001 годзе, пісаў у калектыўным блогу, што меў назву "Gileh Mard" ("Чалавек з Гілану"). У 2002 годзе распачаў свой уласны ўэб-сайт "Pfnjereh Eltehab" ("Акно надзеі") (www.sigarchi.com).

На пачатку 2005 года Сігарчы быў на два месяцы затрыманы Міністэрствам інфармацыі і бясьпекі і асуджаны на 14 гадоў турэмнага зьняволеньня. Зараз на свабодзе, пакуль разглядаецца апэляцыя па ягонай справе.

НЭПАЛ

“Мы распавядаем сьвету пра тое, што тут адбываецца”

Блог “Радыё “Свабодны Нэпал”” (“Radio Free Nepal” (RFN))
http://freenepal.blogspot.com

1 лютага 2005 году. Кароль Нэпала Джанэндра захапіў уладу ў краіне. Народ даведаўся пра гэта з тэлевізійнай прамовы, праслухаўшы якую, я захацеў даведацца пра міжнародную рэакцыю на гэтыя падзеі і паспрабаваў падключыцца да інтэрнэту праз мадэм. Але апэратар паведаміў, што сувязі няма. Я зразумеў, што тэлефонная лінія адключаная.

Каб не дапусьціць распаўсюджваньня любой інфармацыі, якая б крытыкавала яго дзеяньні, кароль загадаў арміі заблякаваць ня толькі інтэрнэт-правайдэраў, але і тэлекамунікацыйную сувязь увогуле.

У той час людзі абмяркоўвалі магчымыя наступствы, некаторыя ўхвалялі дзеяньні караля. У рэдакцыі газэты, дзе я працаваў, усе прадбачылі змрочную будучыню – ваенныя ў студыі тэлевізійных навінаў у якасьці цэнзараў. Тады я падумаў, што правільна было б запісваць, што адбываецца, і што думаюць людзі ў дзёньнік. Я пачаў рабіць гэта на сваім кампутары.

8 лютага тэлекамунікацыйныя паслугі і інтэрнэт сталі даступнымі. Па электроннай пошце я атрымаў мноства лістоў, у якіх людзі пыталіся, што адбываецца ў Нэпале. Тады я падумаў, што лепей за ўсё раскажа пра тыя падзеі мой дзёньнік. Сябры з ЗША параілі мне разьмясьціць дзёньнік, у якім распавядаецца пра падзеі, што ўжо прайшлі, на блогу. Паколькі я быў навічком у блогінгу, сябры самі запусьцілі сайт і разьмясьцілі на ім мае нататкі. Мы вырашылі, што я буду пісаць ананімна і прапаную сябрам у Нэпале таксама пісаць у блогах ананімна, каб пазьбегнуць магчымага перасьледу і турмы.

Вольны доступ да інфармацыі на “RFN” зрабіў сайт папулярным ва ўмовах жорсткай цэнзуры сродкаў масавай інфармацыі. Акрамя таго, Blogger.com раіў наведаць сайт. Мае сябры ў ЗША зрабілі ўсё магчымае для папулярызацыя сайта, і ўжо праз некалькі тыдняў ён быў даволі вядомым.

Я вырашыў распачаць “RFN”, каб людзі ўва ўсім сьвеце даведаліся, што думаюць нэпальцы пра наўпростае кіраваньне караля. Ува ўмовах жорсткай цэнзуры сродкі масавай інфармацыі вымушаныя пісаць тое, што хоча кароль, а ў такіх умовах немагчыма пачуць праўдзівы голас народа. Нягледзячы на тое, што “RFN” – гэта праект аднаго чалавека, (праўда, туды пішуць яшчэ некалькі чалавек), ён найлепшым чынам перадае галасы народа, паколькі свабодны ад цэнзуры і перасьледу.

Раньнія нататкі ў “RFN” былі пераважна апісаньнямі падзей, што адбываліся штодня, як у дзёньніку. Пазьнейшыя – гэта роздумы над рознымі падзеямі і іх аналіз. У палітычнай сытуацыі Нэпала, калі кароль захапіў усю ўладу, пераступіўшы праз выбар народа, роля “RFN” вельмі важная, таму што гэты блог адлюстроўвае думкі простых людзей.

Я хачу, каб у краіне ўсталявалася дэмакратыя, таму што веру, што толькі ў гэтым выпадку краіна стане заможнай, і мая журналісцкая кар’ера будзе мець сэнс. Пісаць ва ўмовах цэнзуры – гэта як піць каву бяз цукру – смак не адчуваецца. Мы, журналісты, даведваемся пра шмат рэчаў, пра якія ня пішуць газэты. Напрыклад, пра тое, што кароль набывае ўласнасьць незаконным шляхам – пра гэта было напісана ў “RFN”. Многія журналісты ведалі пра гэта, крытыкавалі гэта, кпілі з караля, але не маглі пра гэта напісаць.

Другая мэта “RFN” – распавесьці пра сытуацыю ў Нэпале як мага большай колькасьці людзей ува ўсім сьвеце. Калі б не было “RNF”, тысячы людзей не даведаліся б, што адбываецца ў Нэпале. На маю думку, дзякуючы “RFN” многіх людзей пачалі цікавіцца сытуацыяй у Нэпале, што вельмі важна.

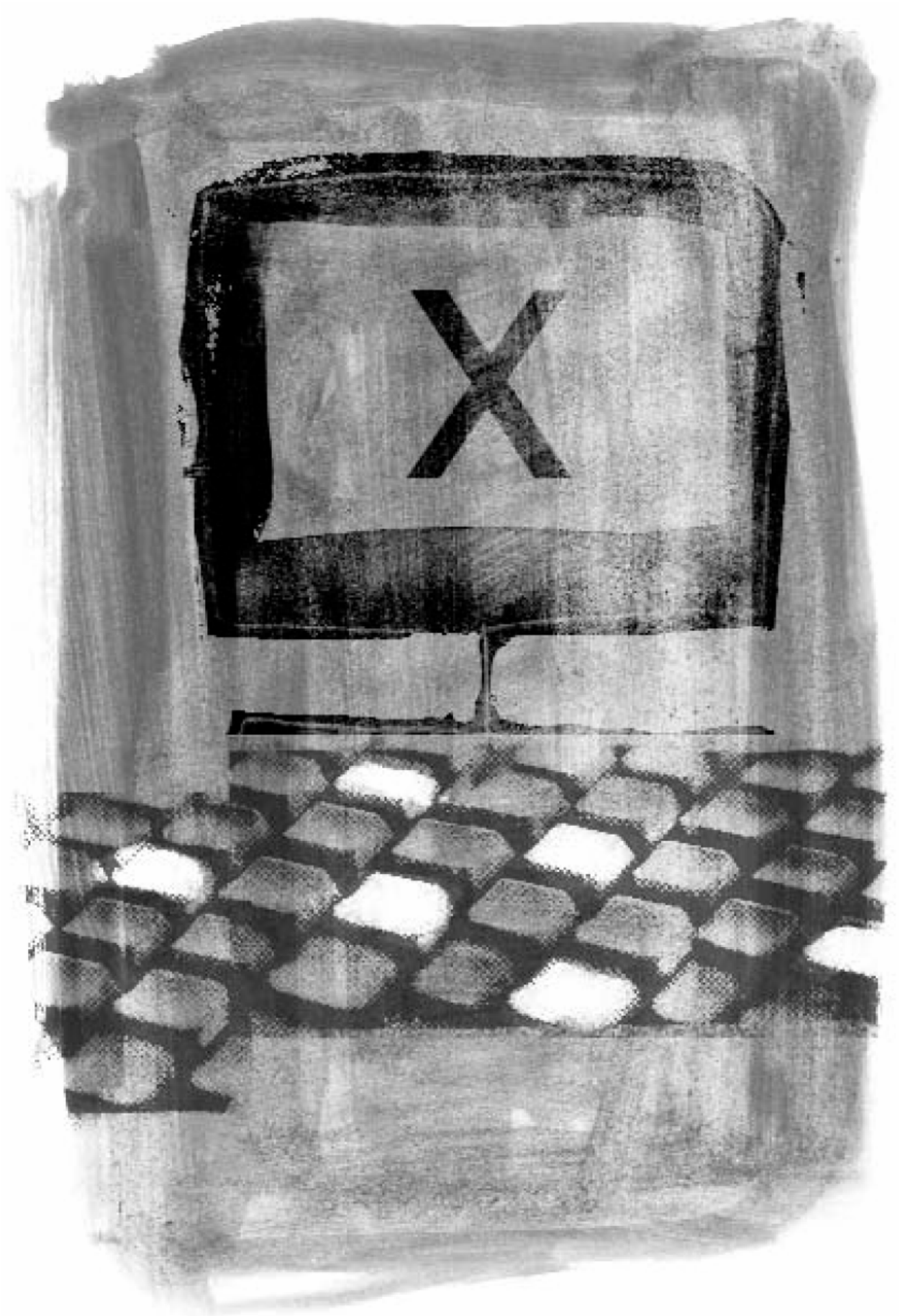
Інфармацыйна-камунікацыйныя тэхналёгіі далі нашаму грамадзтву вельмі шмат. Дзякуючы ім мы пішам свабодна і не баючыся. Напрыклад, я займаюся блогінгам наступным чынам: пішу нататкі і дасылаю іх па электроннай пошце сябру ў ЗША, які іх выстаўляе на сайце. Каб мяне высачыць, трэба прыкласьці немалыя намаганьні. Калі ў маю краіну вернецца дэмакратыя і дасьць нам "паветра, каб вольна дыхаць", я буду ганарыцца сабой, таму што буду адчуваць, што і я зрабіў свой унёсак у гэтую справу.

У мяне часта пытаюцца ў электронных лістах, наколькі мае нататкі вартыя даверу. Я адказваю, што адно толькі імя ня можа быць гарантыяй даверу. Я не хачу падпісваць свае нататкі рэальным імем, таму што пакуль у Нэпале не ўсталюецца дэмакратыя, сытуацыя можа яшчэ больш пагоршыцца і мяне могуць кінуць у турму за блогінг. Я не баюся турмы, але я хачу працягваць рабіць "RFN", каб распавядаць сьвету пра Нэпал. Я адказваю ім, што маё імя стане вядомым, калі скончыцца праўленьне караля.

А пакуль дзякуй усім вам за падтрымку.

RFN Блогер(RFN BLOGGER), Нэпал
wewantdemocracy@gmail.com

"Радыё "Свабодны Нэпал"" (RFN) – гэта блог, выказвае пратэст супраць захопу ўлады ў краіне каралём Джанэндам і цэнзуры сродкаў масавай інфармацыі. "RFN" змагаецца за ўсталяваньне дэмакратыі, гэта сайт, на якім грамадзяне Нэпалу распавядаюць сьвету пра тое, што адбываецца ў іх краіне. Нататкі, разьмешчаныя на сайце, ананімныя, паколькі існуе пагроза перасьледу з боку ўладаў.


X

ЯК ВЕСЬЦІ БЛОГ **АНАНІМНА**

Этан Цукерман (Ethan Zuckerman)

Гэты кароткі тэхнічны дапаможнік па ананімнаму вядзеньню блога – спроба падыйсьці да праблемы з боку чалавека, які паведамляе пра злоўжываньне становішчам членам ўраду, дзейнасьць якога далёка не празрыстая.

Гэты дапаможнік не для кібэрпанкаў, але для людзей з разьвіцьцёвых краін, якія ня ўпэўненыя ў сваёй бясьпецы і хочуць даведацца, як на практыцы забясьпечыць сваю ананімнасьць. Дапаможнік "Як бясьпечна весьці блог" ("How to blog safely"), падрыхтаваны Фондам "Электронная мяжа" ("The Electronic Frontier Foundation") (http://www.eff.org/Privacy/Anonimity/blog-anonymously.php), таксама прапануе шэраг карысных парадаў на гэтую тэму.

ЗЬМЕСТ

Знаёмства з Сарай
Крок 1 Псэўданімы
Крок 2 Агульнадаступныя кампутары
Крок 3 Ананімныя проксі-сэрвэры
Крок 4 Гэтым разам усё надзейна!
Крок 5 Цыбулінная маршрутызацыя (onion routing) праз Tor
Крок 6 MixMaster, Invisiblog і GPG
Якая аптымальная ступень ананімнасьці? Дзе трэба спыніцца?

ЗНАЁМСТВА З САРАЙ

Сара працуе бухгалтаркай ува ўрадавай установе. Яна даведваецца, што яе начальнік, намесьнік міністра, крадзе вялікія сумы грошай у дзяржавы. Яна хоча, каб сьвет даведаўся пра гэтае злачынства, але баіцца згубіць працу. Калі яна паведаміць пра злачынства міністру (калі толькі ў яе атрымаецца да яго прабіцца!), яе могуць звольніць. Яна тэлефануе рэпартэру мясцовай газэты, але той кажа, што для артыкула трэба нашмат болей інфармацыі, а таксама дакумэнты, якія б пацьвярджалі яе падазрэньні.

Такім чынам, Сара вырашае распачаць уэблог, каб расказаць сьвету пра тое, што ёй вядома пра цёмныя справы ў Міністэрстве. Каб абараніць сябе, Сары трэба быць упэўненай, што ніхто ня зможа даведацца, хто яна, з яе нататкаў у блогу. Ёй трэба весьці блог ананімна.

Калі яна распачне ананімны блог, яе можна вылічыць двумя шляхамі. Першы: гэта можна зразумець са зьмесьціва. Напрыклад, калі яна піша: "Я працую памочніцай галоўнага бухгалтара ў апараце міністра вугальнай прамысловасьці", даволі хутка можна даведацца яе імя. Другі: на падставе інфармацыі, атрыманай праз уэб-браўзэры і паштовыя праграмы. Кожны кампутар, падключаны да інтэрнэту, мае свой асобны ці сумесны IP-адрас. Гэта набор з чатырох нумароў ад 0 да 255, аддзеленых кропкамі, напрыклад: 213.24.124.38. Калі Сара разьмяшчае свае нататкі ў інтэрнэце з дапамогай уэб-браўзэра з працоўнага кампутара, то IP адрас уключаецца ў яе паведамленьне.

Не прыклаўшы вялікіх намаганьняў, кампутаршчыкі ў міністэрстве высьветляць асобу Сары па гэтым IP адрасе.
Сара вырашае зьвязацца з правайдэрам інтэрнэт-паслуг (ISP) з дапамогай мадэма з дамашняга кампутара. Але кожны правайдэр фіксуе, які IP адрас меў канкрэтны

тэлефонны нумар у дадзены час. У адных краінах міністру будзе патрэбны сьпецыяльны дазвол на атрыманьне такой інфармацыі, у іншых (асабліва там, дзе доступ да інтэрнэту прадастаўляецца дзяржаўнымі кампаніямі, такую інфармацыю атрымаць вельмі проста. Тады ў Сары будуць праблемы.

Існуе шэраг спосабаў, як Сара можа захаваць ананімнасьць, карыстаючысі інтэрнэтам. Як правіла, чым у большай бясьпецы хоча быць чалавек, тым больш працы яму давядзецца правесьці. Сары, і кожнаму іншаму чалавеку, што хоча займацца блогінгам ананімна, неабходна вызначыцца, наколькі вялікая яе (яго) параноя, перш чым вырашыць, колькі намаганьняў прыкласьці да таго, каб захаваць сваю ананімнасьць. Як вы пабачыце далей, некаторыя стратэгіі захаваньня ананімнасьці патрабуюць шмат тэхнічных ведаў і працы.

КРОК 1 – ПСЭЎДАНІМЫ

Самы просты спосаб, каб забясьпечыць ананімнасьць Сары - гэта выкарыстоўваць бясплатныя інтэрнэт-пошту і блогавую плятформу па-за межамі краіны, у якой яна жыве. (Карыстацца платнымі паслугамі для электроннай пошты і інтэрнэту ня варта, таму што па нумары рахунка ці крэдытнай карты можна вызначыць імя карыстальніка). Сара можа стварыць сабе новае імя – псэўданім, якім будзе карыстацца ў сеціве. І калі міністар знойдзе яе блог, ён пабачыць імя аўтара: "Y.N.Ymous" і яго электронны адрас anonymous.whistleblower@hotmail.com.

Вось некарорыя з правайдэраў бясплатных паштовых паслугаў:
Hotmail
Yahoo
Hushmail – бясплатная пошта з добрай крыптаграфічнай абаронай

Некаторыя з правайдэраў бясплатнага хостынгу для блогаў:
Blogsome – бясплатныя WordPress блогі
Blogger
Seo Blog

Аднак тут паўстае праблема стратэгіі. Калі Сара падпісваецца на бясплатную электронную пошту ці бясплатную блогавую плятформу, уэб-сэрвэр, які яна выкарыстоўвае, рэгіструе яе IP адрас. Калі з дапамогай гэтага IP адрасу яе адсочаць – калі яна карыстаецца дамашнім ці працоўным кампутарам – і калі кампанію, што прапануе паслугі пошты ці блогінгу прымусяць паведаміць гэтую інфармацыю, то Сару лёгка знойдуць. Прымусіць большасьць кампаній, што прапануюць паслугі па карыстаньні сецівам, выдаць такую інфармацыю ня так проста. Напрыкалад, каб прымусіць Hotmail раскрыць IP адрас, якім карысталася Сара пры падключэньні, міністру, хутчэй за ўсё, спатрэбіцца спэцыяльны дазвол, па які, магчыма, давядзецца зьвярнуцца да праваахоўных органаў ЗША. Але Сара, магчыма, не захоча рызыкаваць, калі ўлады ў яе краіне могуць пераканаць інтэрнэт-кампаніі, паслугамі якіх яна карысталася, паведаміць інфармацыю пра яе.

КРОК 2 – АГУЛЬНАДАСТУПНЫЯ КАМПУТАРЫ

Каб захаваць ананімнасьць, Сара можа займацца блогінгам на кампутарах, якімі карыстаецца вялікая колькасьць людзей. Зарэгістраваць сваю пошту ці блог яна можа з кампутара ў інтэрнэт-кавярні, бібліятэцы ці ва ўнівэрсытэцкай інтэрнэт-лябараторыі. Калі міністар даведаецца IP адрас аўтара нататкаў ці камэнтароў, ён пабачыць, што паведамленьне дасланае з інтэрнэт-кавярні з кампутара, на якім магло працаваць невядома колькі людзей.

У гэтай стратэгіі таксама ёсьць свае слабыя месцы. Напрыклад, калі ў інтэрнэт-кавярні ці кампутарнай лябараторыі фіксуюецца, хто і ў які час карыстаўся якім кампутарам. У такім выпадку Сару лёгка знайсьці. Ёй ня варта прыходзіць у лябараторыю ўначы, калі там нікога няма, таму што лябарант лёгка яе запомніць. Ёй трэба часта мяняць інтэрнэт-кавярні. Калі

міністар высьветліць, што ўсе паведамленьні дасланыя з інтэрнэт-кавярні "Joe's Beer and Bits" з Мэйн стрыт , ён можа пачаць сачыць за кавярняй і знойдзе Сару.

КРОК 3 – АНАНІМНЫЯ ПРОКСІ-СЭРВЭРЫ

Сары надакучыла хадзіць у інтэрнэт-кавярню кожны раз, калі ёй трэба абнавіць блог. З дапамогай суседа-кампутаршчыка яна атрымала доступ да інтэрнэту праз ананімны проксі-сэрвэр з дамашняга кампутара. Цяпер, калі яна карыстаецца электроннай поштай ці займаецца блогінгам, яна пакідае IP адрас проксі-сэрвэра, а не адрас дамашняга кампутара, і мінстру будзе вельмі цяжка яе знайсьці.
Па-першае, яна знаходзіць у пошукавіку Google сьпіс проксі-сэрвэраў ("proxy server") і выбірае проксі-сэрвэр са сьпісу publicproxyservers.com.list, пазначаны надпісам "high anonymity" ("высокая ступень ананімнасьці"). Яна выпісвае са сьпісу IP адрас проксі і порта.

Вось некалькі надзейных сьпісаў адкрытых проксі-сэрвэраў:

- publicproxyservers.com – ананімныя і неананімныя проксі-сэрвэры;
- Samair (http://www.samair.ru/proxy/) – выключна ананімныя проксі-сэрвэры, а таксама інфармацыя пра проксі-сэрвэры, якія падтрымліваюць SSL;
- Rosinstrument proxy database (http://tools.rosinstrument.com/proxy/) – пошук па базе дадзеных проксі-сэрвэраў).

Потым Сара пераходзіць у разьдзел "preferences" свайго ўэб-пошукавіка. У разьдзелах "general", "network" ці "security" (звычайна) яна знаходзіць опцыю атрыманьня доступу да інтэрнэту праз проксі-сэрвэр. (У пошукавіку Firefox гэтая опцыя знаходзіцца пад Preferences – General - Connection Settings).

Сара ўключае "ручную настройку проксі-сэрвэра ("manual proxy configurations"), уводзіць IP адрас проксі-сэрвэра і порта ў палі для HTTP proxy і SSL proxy і захоўвае свае парамэтры. Яна перазагружае свой браўзэр і пачынае працаваць у інтэрнэце.

Сара заўважае, што сувязь запаволілася. Гэта адбываецца таму, што кожная старонка, на якую яна дае запыт, загружаецца абыходным шляхам. Замест непасрэднага падключэньня да hotmail.com, кампутар злучаецца з проксі-сэрвэрам, і той падключаецца да Hotmail. Старонка, якую Hotmail дасылае Сары, спачатку ідзе на проксі-сэрвэр, а толькі потым да Сары. Яна таксама заўважае, што ўзьніклі цяжкасьці з доступам да ўэб-сайтаў, асабліва да тых, якія патрабуюць рэгістрацыі. Але затое яе IP адрас невядомы правайдэру.

Можна правесьці з проксі-сэрвэрамі цікавы экспэрымэнт: зайдзіце на noreply.org – папулярны сайт, які займаецца перасылкай ("remailer"). На маніторы зьявіцца прывітаньне з вашым IP адрасам: "Hello pool-151-203-182-212.wma.east.verizon.net 151.203.182.212, pleased to meet you".

Цяпер ідзіце на anonymizer.com , які дазваляе бачыць некаторыя ўэб-старонкі праз ананімны проксі. У акно ў правым верхнім куце старонкі ўвядзіце URL для http://www.noreply.org (ці проста націсьніце на спасылку [http://anon.free.anonymizer.com/http://www.noreply.org]. Вам стане зразумела, што noreply.com цяпер лічыць, што вы прыйшлі з vortex.anonymizer.com.(Anonymizer – гэта добры спосаб, каб праверыць проксі-сэрвэры, не зьмяняючы парамэтры ў настройцы вашага браўзэра, але гэта не працуе з больш дасканалымі сэрвэрамі, такімі, як webmail ці weblogging).

І, нарэшце, выконвайце інструкцыі, прыведзеныя вышэй, каб настроіць свой уэб-браўзэр на выкарыстаньне ананімнага проксі-сэрвэра, пасьля чаго наведайце noreply.org, каб даведацца, ці зафіксаваў ён ваш IP адрас.

На жаль, проксі-сэрвэры таксама недасканалыя. Калі ў краіне, дзе жыве Сара, дзейнічаюць законы, якія абмяжоўваюць карыстаньне інтэрнэтам, многія карыстальнікі

будуць выкарыстоўваць проксі-сэрвэры, каб атрымаць доступ да сайтаў, заблякаваных уладамі. Улады могуць у адказ заблякаваць найбольш папулярныя проксі-сэрвэры. Карыстальнікі будуць пераходзіць да новых проксі-сэрвэраў, якія ўлады таксама праз нейкі час заблякуюць, і так па крузе. Праз гэта на пошукі і зьмены проксі-сэрвэраў можна згубіць вельмі шмат часу. Сара можа мець іншую праблему, калі яна адна з нямногіх у сваёй краіне, хто карыстаецца паслугамі проксі-сэрвэраў. Калі яе блог абнаўляецца з аднаго і таго ж проксі-сэрвэра, і калі міністру ўдасца атрымаць рэгістрацыйныя запісы ад усіх інтэрнэт-праваўдэраў (ISPs), што дзейнічаюць у краіне, ён зможа высьветліць, што кампутар Сары – адзін зь нямногіх кампутараў, што зьвязваліся з канкрэтным проксі-сэрвэрам. Ён ня зможа даказаць, што Сара карысталася проксі-сэрвэрам, каб дасылаць абнаўленьні на блог, але ён можа зрабіць высновы, што калі проксі-сэрвэр выкарыстоўвалі, каб даслаць абнаўленьне на блог, і што Сара – адна зь нямногіх людзей у краіне, што карысталіся гэтым проксі-сэрвэрам, то яна – аўтарка гэтага блогу. Таму Сары трэба карыстацца папулярнымі ў яе краіне проксі-сэрвэрамі і часта мяняць іх.

КРОК 4 – ГЭТЫМ РАЗАМ УСЁ НАДЗЕЙНА!

Сара пачынае баяцца, што проксі-сэрвэры, якімі яна карыстаецца, яе выдадуць. Што, калі міністар прымусіць апэратара проксі-сэрвэра (дасьць яму хабар ці націсьне на яго з дапамогай закона) фіксаваць, хто ў яго краіне карыстаецца проксі-сэрвэрам, а таксама якія сайты гэтыя людзі наведваюць. Сара спадзяецца, што адміністратар проксі-сэрвэра яе абароніць, але яна нават ня ведае, хто ён такі. Адміністратар можа нават і ня ведаць, што яна карыстаецца проксі-сэрвэрам, але проксі-сэрвэры часта адчыняюцца выпадкова.

У Сары ёсьць сябры ў Канадзе (у гэтай краіне інтэрнэт не цэнзуруецца так, як у яе на радзіме), якія могуць пагадзіцца дапамагаць ёй весьці блог, захоўваючы яе ананімнасьць. Сара тэлефануе свайму сябру і просіць, каб ён усталяваў на сваім кампутары "Circumventor". "Circumventor" – гэта адзін зь дзясяткаў проксі-сэрвэраў, якія вы можаце ўстляваць на свой кампутар. Гэта дазволіць іншым людзям выкарыстоўваць ваш кампутар у якасьці проксі-сэрвэра.

Джым, сябра Сары, загружае Circumventor (http://www.peacefire.org/circumventor/simple-circumventor-instructions.html) з Peacefire.org і ўсталёўвае яго на сваю Windows сыстэму. Гэта зрабіць няпроста: яму трэба ўсталяваць Perl, потым OpenSA і толькі пасьля іх Circumventor. Акрамя таго, трэба, каб кампутар Джыма увесь час быў падключаны да інтэрнэту, каб Сара магла выкарыстоўваць яго як проксі-сэрвэр, і каб яна не прасіла Джыма кожны раз, калі ёй трэба даслаць матэрыял, падключыцца да інтэрнэту. Джым усталёўвае праграмнае забесьпячэньне, тэлефануе Сары на мабільны тэлефон і паведамляе URL, якім яна будзе карыстацца, каб падключыцца да інтэрнэту ці абнавіць свой блог з дапамогай проксі-сэрвэра Джыма. Гэта зручна яшчэ і тым, што Сара можа карыстацца проксі-сэрвэрам Джыма як дома, так і ў інтэрнэт-кавярні, і ёй ня трэба нічога мяняць у сваім кампутары.

Сара, безумоўна, вельмі ўдзячная Джыму за дапамогу, але тут, усё ж, існуе адна арганізацыйная праблема. Кампутар Джыма (які працуе з сыстэмай Windows) часта перазагружаецца. Кожны раз, калі гэта адбываецца, правайдэр (ISP) прысвойвае машыне новы IP адрас і проксі-сэрвэр перастае працаваць для Сары. Джыму трэба зьвязвацца з Сарай зноўку, каб паведаміць новы IP адрас. Гэта нязручна і дорага. Сару непакоіць і тое, што калі яна доўгі час будзе карыстацца нейкім адным IP адрасам, яе правайдэр можа паддацца ціску з боку ўладаў і заблякаваць гэты адрас.

КРОК 5 – ЦЫБУЛІННАЯ МАРШРУТЫЗАЦЫЯ ПРАЗ TOR (ONION ROUTING THROUGH TOR)

Джым прапануе Сары паэкспэрымэнтаваць з Tor – адносна новай сыстэмай, якая забясьпечвае высокую ступень ананімнасьці карыстальнікам інтэртэту. "Цыбулінная маршрутызацыя" ("onion routing") падымае на новы ўзровень складанасьці ідэю проксі-сэрвэраў (кампутар, якія дзейнічае ад вашага імя). Кожны запыт, зроблены праз сетку "цыбуліннай маршрутызацыі", праходзіць празь некалькі дадатковых кампутараў (якіх можа

быць ад двух да дваццаці). У выніку вельмі цяжка прасачыць, зь якога кампутара быў дасланы запыт.

Кожны крок у ланцугу "цыбуліннай маршрутызацыі" зашыфраваны. Дзякуючы гэтаму ўладам у краіне, дзе жыве Сара, будзе цяжэй адсачыць яе блог. Болей таго, кожны кампутар у ланцугу ведае толькі бліжэйшых суседзяў. Іншымі словамі, маршрутызатар B ведае, што адтрымаў запыт на ўэб-старонку ад маршрутызатара A, і што яму неабходна перадаць запыт маршрутызатару C. Але і сам запыт зашыфраваны – маршрутызатар B насамрэч ня ведае, што гэта за старонка, на якую Сара даслала запыт, ці які маршрутызатар апошні ў ланцугу.

Ведаючы пра складанасьць тэхналёгіі, Сара прыемна зьдзіўленая лёгкасьцю ўсталяваньня сыстэмы "цыбуліннай маршрутызацыі" Tor (http://tor.eff.org/docs/tor-doc-win32.html.en). Яна загружае праграму, якая ўсталёўвае Tor на яе кампутар, потым загружае і ўсталёўвае Privoxy – проксі-сэрвэр, які працуе з Tor і мае дадатковую выгоду таму што аўтаматычна прыбірае рэкляму з уэб- старонак, якія праглядае Сара.

Пасьля ўсталяваньня праграмнага забесьпячэньня і перазагрузкі кампутара Сара заходзіць на noreply.org і бачыць, што яна пасьпяхова "замаскаваная" сыстэмай Tor – noreply.org думае, што яна падключаецца з Гарвардзкага ўнівэрсытэта. Сара перазагружае кампутар - зараз noreply думае, што яна ў Нямеччыне. Сара робіць выснову, што Tor з кожным запытам зьмяняе яе адрас, дапамагаючы ёй захаваць ананімнасьць.

Аднак гэта мае некалькі непрыемных наступстваў. Калі Сара падключаецца да Google праз Tor, пачынаюць пераключацца мовы. Адзін пошук – на ангельскай мове, другі – на японскай, далей на нямецкай, дацкай ці галяндзкай – усё гэта на працягу некалькіх хвілін. Сара ня супраць вывучыць новую мову, але яе непакояць іншыя наступствы. Сары падабаецца пісаць для Wikipedia, але высьвятляецца, што Wikipedia блякуе яе спробы рэдагаваць артыкулы, калі яна карыстаецца Tor.

Выглядае, што з Tor – тыя ж самыя праблемы, што і зь іншымі проксі-сэрвэрамі. Хуткасьць працы ў інтэрнэце запавольваецца, у параўнаньні з працай бяз проксі-сэрвэраў. Сара пачынае карыстацца Tor толькі калі хоча даслаць абнаўленьне на блог ці наведаць забаронены сайт. Зноўку ж яна прывязаная да дамашняга кампутара, таму што вельмі цяжка ўсталяваць Tor на кампутары грамадзкага карыстаньня.

Але болей за ўсё Сару непакоіць тое, што час ад часу Tor перастае працаваць. Відавочна, што яе правайдэр блякуе некаторыя маршрутызатары "цыбуліны" – Tor спрабуе злучыцца з заблякаваным маршрутызатарам, але нават пасьля некалькіх хвілін чаканьня патрэбная старонка так і не адчыняецца.

КРОК 6 – MIXMASTER, INVISIBLOG І GPG

Безумоўна, праблему блогінгу можна вырашыць і без выкарыстаньня проксі-сэрвэраў, нават такіх дасканалых, як Tor.

Пасьля шматлікіх кансультацый зь мясцовымі кампутарнымі спэцыялістамі Сара спрабуе новы варыянт: invisiblog (http://www.invisiblog.com/). Гэта сайт ананімнай групы аўстралійцаў, які мае назву vigilant.tv – створаны параноікамі і для параноікаў. На Invisiblog немагчыма дасылаць свае матэрыялы праз сеціва (як гэта робіцца з большасьцю блогінгавых сэрвэраў), але па электроннай пошце адмысловага фармату, праз рымэйлерную сыстэму MixMaster, якая мае крыптаграфічны подпіс.

Сара зрабіла некалькі спробаў, перш чым зразумела сэнс апошняга сказа. У рэшце рэшт, яна ўсталявала GPG (http://www.gnupg.org/) - GNU вэрсію "Pretty Good Privacy" ("Дастатковая ступень ананімнасьці"). Гэта сыстэма шыфроўкі з адкрытым ключом (http://en.wikipedia.org/wiki/Public-key_cryptography).

Коратка гэта можна патлумачыць наступным чынам: шыфроўка з "адкрытым" ключом – гэты тэхніка, якая дазволіць Сары дасылаць паведамленьні нейкай асобе, якія можа прачытаць толькі яна; яна не паведамляе вам свой "закрыты"ключ, каб вы не змаглі прачытаць паведамленьні, якія іншыя людзі дасылаюць ёй. Шыфроўка з "адкрытым" ключом таксама дазваляе "ставіць лічбавы подпіс" пад дакумэнтам, які амаль немагчыма падрабіць.

Сара стварае пару ключоў, якія яна будзе выкарыстоўваць, дасылаючы абнаўленьні на свой блог і падпісваючыся пад нататкамі з дапамогай "закрытага" ключа. Блог-сэрвэр зможа з дапамогай яе "адкрытага" ключа спраўдзіць, ці нататкі даслала менавіта яна, пасьля чаго разьмесьціць іх на блогу. (глядзіце таксама разьдзел "Як забясьпечыць прыватнасьць электроннай пошты".)

Потым Сара ўсталёўвае MixMaster – паштовую сыстэму, створаную для таго, каб хаваць паходжаньне электроннага паведамленьня. MixMaster выкарыстоўвае ланцуг ананімных рымэйлераў – кампутарных праграм, якія прыбіраюць усю апазнавальную інфармацыю з электроннага паведамленьня і перасылаюць яго адрасату. Гэта робіцца для забесьпячэньня высокай ступені ананімнасьці. Калі выкарыстоўваецца ад двух да дваццаці рымэйлераў, вельмі цяжка адсачыць паведамленьне, нават калі адзін ці болей рымэйлераў "падкупленыя" і запісваюць інфармацыю пра аўтара паведамленьня. Для таго, каб "пабудаваць" MixMaster, Сары трэба сабраць яго першапачатновы код. У гэтай справе ёй спатрэбіцца дапамога кампутарнага спэцыяліста.

Сара дасылае першае MixMaster паведамленьне, разам з "адкрытым" ключом, на Invisiblog. Invisiblog выкарыстоўвае гэта, каб стварыць новы блог з мудрагелістай назвай "invisiblog.com/ac4589d7001ac238" – ланцуг з шаснаццаці апошніх байтаў GPG ключа Сары. Наступныя паведамленьні Сара дасылае на Invisiblog такім чынам: піша тэкст паведамленьня, падпісвае яго сваім "адкрытым" ключом і адпраўляе яго праз MixMaster.

Хуткасьць блогінгу пры гэтым значна запавольваецца. Паколькі MixMaster перанакіроўвае паведамленьне (заблытавае шляхі), паведамленьне ідзе да сэрвэраў ад двух гадзін да двух дзён. Сары таксама трэба быць асьцярожнай і не заходзіць на блог у якасьці наведніка занадта часта, бо ў такім выпадку яе IP адрас зьявіцца ў сьпісе частых наведнікаў блогу, з чаго можна зрабіць выснову, што яна - аўтарка блогу. Але Сара супакойвае сябе тым, што ўладальнікі Invisiblog ня ведаюць, хто яна.

Асноўная праблема з сыстэмай Invisiblog – гэта тое, што яе выкарыстаньне вельмі складанае для большасьці людзей. Для іх усталяваньне GPG – гэта вялікая праблема, і ім таксама цяжка зразумець усе складанасьці "адкрытага" і "закрытага" ключоў. Нават сыстэмы крыптаграфіі, створаныя для звычайных карыстальнікаў, такія, як, напрыклад, Ciphire, не такія простыя. У выніку, вельмі мала людзей, нават сярод тых, каму гэта неабходна, выкарыстоўваюць шыфраваньне для большай часткі сваёй электроннай карэспандэнцыі.

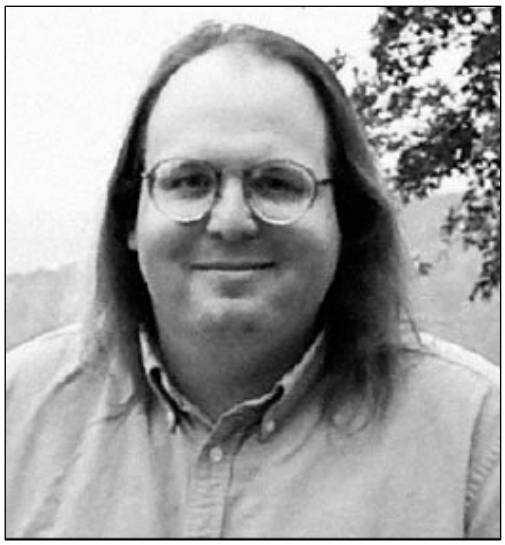
MixMaster – тэхнічна цяжкая задача для большасьці карыстальнікаў. Карыстальнікі Windows могуць зьвярнуцца да раньняй DOS-вэрсыі праграмы, якую можна загрузіць з: http://prdownloads.sourceforge.net/mixmaster/mix204b46.zip?download. Я загрузіў і паспрабаваў яе, але яна чамусці не працуе... магчыма, маё паведамленьне дагэтуль перасылаецца ад рымэйлера да рымэйлера. Таму, хто хоча паспрабаваць больш новую вэрсію ці праграму на Linux ці Mac, трэба пісаць праграмы самім, а гэтая задача не пад сілу нават шмат якім вопытным карыстальнікам. Магчыма, Invisiblog стане больш даступным, калі пачне прыймаць паведамленьні ад рымэйлераў, даступных праз сеціва, напрыклад, такіх, як riot.eu.org. Але пакуль наўрадці ён дапаможа тым, каму ён сапраўды патрэбен.

У краінах з рэпрэсіўным рэжымам існуе яшчэ адна праблема з моцным шыфраваньнем. Калі ўлады канфіскуюць кампутар Сары і знойдуць яе "закрыты" ключ, гэта будзе сур'ёзным доказам таго, што Сара - аўтарка "падрыўных" матэрыялаў на блогу. У краінах, дзе шыфраваньне шырока не выкарыстоўваецца, проста адправіць паведамленьне праз

MixMaster, дзе яно моцна шыфруецца, можа быць дастаткова для таго, каб за дзейнасьцю Сары ў інтэрнэце пачалі сачыць.

ЯКАЯ АПТЫМАЛЬНАЯ СТУПЕНЬ АНАНІМНАСЬЦІ? ДЗЕ ТРЭБА СПЫНІЦЦА?

Ці падыходзіць вам рашэньне Сары: атрымаць дадатковыя веды пра шыфраваньне і праграмнае забесьпячэньне, каб выкарыстоўваць MixMaster? Ці, можа, вам дастаткова скамбінаваць крокі 1-5, каб займацца блогінгам ананімна? Адназначнага адказу няма. Пры выбары спосабу, з дапамогай якога захоўваць ананімнасьць, неабходна ўлічваць мясцовыя ўмовы, вашу тэхнічную падрыхтоўку, а таксама ступень вашай параноі. Калі вы лічыце, што весьці блог рызыкоўна, і што вам пад сілу ўсталяваць Tor, то гэта вельмі добрае рашэньне праблемы.



І памятайце: ня варта падпісваць нататкі на блогу вашым сапраўдным імем!

Этан Цукерман – супрацоўнік Цэнтра імя Бэркмана "Інтэрнэт і грамадзтва" на юрыдычным факультэце Гарвардзкага ўнівэрсытэта (the Berkman Center for Internet and Society at Harward Law School). Тэма яго дасьледаваньняў – адносіны паміж грамадзянскай журналістыкай і традыцыйнымі мэдыямі, галоўным чынам, у разьвіцьцёвых краінах. Ён – заснавальнік і былы дырэктар "Geekcorps" – НДА, якая праводзіць трэнінгі па авалоданьні кампутарнымі тэхналёгіямі ў разьвіцьцёвых краінах. Этан Цукерман – адзін з заснавальнікаў хостынгавай кампаніі Tripod.

ТЭХНІЧНЫЯ ПАРАДЫ, ЯК **АБЫЙСЬЦІ ЦЭНЗУРУ**

Нарт Віленёв (Nart Villeneuve)

ЗЬМЕСТ

- **ФІЛЬТРАЦЫЯ ЗЬМЕСЬЦІВА ІНТЭРНЭТУ**
- **ТЭХНАЛЁГІІ АБЫХОДУ**
- **АЦЭНКА ПАТРЭБАЎ І МАГЧЫМАСЬЦЯЎ**
- **УЭБ-ТЭХНАЛЁГІІ АБЫХОДУ:**
  - Агульнадаступныя онлайнавыя паслугі
  - Праграмнае забесьпячэньне
  - Пытаньні бясьпекі
- **ПРОКСІ-СЭРВЭРЫ:**
  - Праграмнае забесьпячэньне
  - Агульнадаступныя проксі-сэрвэры
  - Лякалізацыя адкрытых проксі-сэрвэраў
  - Адкрытыя проксі-сэрвэры: нестандартныя порты
- **ПЫТАНЬНІ БЯСЬПЕКІ**
- **ТУНЭЛЯВАНЬНЕ**
- **АНАНІМНЫЯ СЫСТЭМЫ КАМУНІКАЦЫЙ**
- **ВЫСНОВЫ**

ФІЛЬТРАЦЫЯ ЗЬМЕСЬЦІВА ІНТЭРНЭТУ

Тэхналёгіі фільтрацыі дазваляюць кантраляваць доступ да зьмесьціва інтэрнэту. Нягледзячы на тое, што першапачаткова тэхналёгіі фільтрацыі распрацоўваліся для індывідуальных патрэбаў (каб бацькі маглі абмяжоўваць доступ дзецям да непажаданага зьмесьціва) цяпер тэхналёгіі фільтрацыі шырока выкарыстоўваюцца шматлікімі арганізацыямі і дзяржаўнымі структурамі. Кантроль доступу да інтэрнэт-зьмесьціва робіцца прыярытэтам для шэрагу арганізацый і ўстаноў, у тым ліку, школаў, біблятэк і карпарацый. Тэхналёгіі фільтрацыі ўсё шырэй выкарыстоўваюцца на дзяржаўным узроўні. Усё насельніцтва краіны можа быць пазбаўлена доступу да пэўнага інтэрнэт-зьмесьціва, часта без тлумачэньняў, чаму.

Тэхналёгіі фільтрацыі зьмесьціва базуюцца на блякіроўцы па сьпісе, часта супольна з тэхналёгіямі блякіроўкі, у якіх выкарыстоўваецца падбор ключавых словаў. Усё гэта дазваляе аўтаматычна блякаваць зьмесьціва. Спачатку складаюцца сьпісы назваў дамэнаў і адрасоў , потым іх сыстэматызуюць і загружаюць ў фільтруючае праграмнае забесьпячэньне, якое можна настроіць на блякіроўку пэўных катэгорый. Калі карыстальнікі спрабуюць адчыніць уэб-старонку, праграма фільтрацыі зьвяртаецца да сьпіса, што знаходзіцца ў базе дадзеных, і блякуе доступ да ўсіх уэб-старонак у гэтым сьпісе. Калі актываваная блякіроўка па ключавым слове, праграма правярае кожную ўэб-старонку (дамэн, URL шлях і (альбо) асноўную частку зьмесьціва старонкі) і аўтаматычна блякуе доступ да ўэб-старонкі, калі знойдзе хаця б адно забароненае ключавое слова.

Сыстэмы фільтрацыі маюць два недахопы: залішняя блякіроўка і недастатковая блякіроўка. Часта яны блякуюць доступ да няправільна клясыфікаванага зьмесьціва, альбо толькі часткова блякуюць доступ да зьмесьціва.

Аднак асноўная праблема – гэта сакрэтнасьць складаньня сьпісаў уэб-сайтаў, якія блякуюцца з дапамогай тэхналёгій фільтрацыі. Нягледзячы на існаваньне адкрытых сьпісаў (звычайна гэта сьпісы парнаграфічных сайтаў), сьпісы камэрцыйных фільтраў, а таксама сьпісы, якія складаюцца на дзяржаўным узроўні, засакрэчаныя. Камэрцыйныя сьпісы падзеленых на катэгорыі дамэнаў і адрасоў зьяўляюцца інтэлектуальнай уласнасьцю вытворцаў і захоўваюцца ў тайне. Нягледзячы на тое, што некаторыя вытворцы праграмнага забесьпячэньня для фільтрацыі адчыняюць доступ да онлайнавых праграм фільтрацыі URL, сьпісы сайтаў, якія блякуюцца, застаюцца засакрэчанымі і недаступнымі для незалежнага назіраньня і аналізу.

Часта ўрады краін пашыраюць камэрцыйныя сьпісы фільтрацыі за кошт пэўных уэб-сайтаў, якія маюць дачыненьне да гэтых краін. У сьпісы сайтаў, што блякуюцца, часьцей за ўсё патрапляюць сайты апазыцыйных палітычных партый ці газэт, праваахоўных арганізацый, міжнародных агенцтваў навінаў, а таксама сайты, што крытыкуюць улады. У большасьці краін пераважна фільтруецца зьмесьціва на мясцовай мове (на англамоўныя сайты не зьвяртаецца вялікай увагі), а таксама сайты, на якіх вядуцца дыскусіі, у прыватнасьці, блогі і ўэб-форумы.

ТЭХНАЛЁГІІ АБЫХОДУ

У адказ на ажыцьцяўленьне фільтрацыі і кантролю зьмесьціва інтэрнэту ўрадамі краін, зьявілася шмат розных тэхналёгій абыходу ("circumvention technologies"). Сутнасьць тэхналёгій абыходу заключаецца ў тым, што запыт карыстальніка з краіны, дзе ажыцьцяўляецца фільтрацыя, накіроўваецца на машыну-пасярэднік, якая не блякуецца. У сваю чаргу, гэты кампутар знаходзіць патрэбную інфармацыю і дасылае яе карыстальніку, які зрабіў запыт. Часам такія тэхналёгіі спэцыяльна распрацоўваюцца для нейкай канкрэтнай сытуацыі ці адаптуюцца да канкрэтнай краіны. У астатніх выпадках карыстальнікі могуць проста адаптаваць да абыходу тэхналёгіі, якія першапачаткова распрацоваліся ў іншых мэтах.

Адныя з гэтых тэхналёгій распрацаваныя прыватнымі кампаніямі, іншыя – групамі хакераў і актывістаў, якія зьбіраліся менавіта з гэтай мэтай. Праграмы могуць уяўляць сабой як простыя скрыпты ("scripts"), так і вельмі складаныя сеткавыя пратаколы. Улічваючы разнастайнасьць тэхналёгій, патэнцыйным карыстальнікам неабходна ўзважыць усе недахопы і перавагі асобных спосабаў і тэхналёгій, каб выбраць тыя, што найбольш адпавядаюць іх патрэбам.

У ажыцьцяўленьні тэхналёгіі абыходу ўдзельнічаюць два бакі: правайдэр абыходу і карыстальнік абыходу. Правайдэр абыходу ўсталёўвае праграмнае забесьпячэньне на кампутар, які знаходзіцца па-за зонай фільтрацыі, і аказвае такую паслугу карыстальнікам інтэрнэту ў рэгіёнах, дзе ажыцьцяўляецца фільтрацыя. Такім чынам, пасьпяховы абыход залежыць ад таго, ці будуць інтарэсы правайдэра адпавядаць інтарэсам карыстальніка.

Гэты артыкул мае мэтай праінфармаваць карыстальнікаў, якія вырашылі зьвярнуцца да тэхналёгій абыходу, пра магчымасьці тэхналёгій, пра тое, як іх выкарыстоўваць і як выбраць тое, што найбольш адпавядае іх патрэбам. Гэта робіцца шляхам вызначэньня патрэбаў і магчымасьцяў тых, хто будзе выкарыстоўваць гэтыя тэхналёгіі – правайдэраў і карыстальнікаў пры захаваньні балянсу паміж патрэбным узроўнем бясьпекі і зручнасьцю тэхналёгіі для карыстальніка. Эфэктыўнасьць, надзейнасьць і стабільнасьць абыходу залежаць ад таго, ці правільную тэхналёгію выбраў карыстальнік.

АЦЭНКА ПАТРЭБАЎ І МАГЧЫМАСЬЦЯЎ

Тэхналёгіі абыходу часта разьлічаныя на розныя катэгорыі карыстальнікаў - у залежнасьці ад магчымасьцяў і вопыту. Тое, што працуе ў адной сытуацыі, не працуе ў іншай. Пры выбары тэхналёгіі абыходу патэнцыйным правайдэру і карыстальніку трэба адказаць на наступныя пытаньні:

Колькі будзе карыстальнікаў і якой будзе прапускная здольнасьць каналаў (для правайдэра і карыстальніка)?

Дзе знаходзіцца галоўны пункт доступу патэнцыйнага карыстальніка да інтэрнэту і для чаго ён будзе выкарыстоўвацца?

Які ўзровень тэхнічнай падрыхтоўкі маюць правайдэр і карыстальнік?

Ці мае карыстальнік надзейныя кантакты па-за межамі яго краіны?

Якое пакараньне пагражае карыстальніку, калі стане вядома, што ён выкарыстоўвае тэхналёгіі абыходу?

- Ці ўсьведамляе карыстальнік магчымую пагрозу ягонай бясьпецы, калі пойдзе на рызыку выкарыстаньня тэхналёгій абыходу?

КОЛЬКАСЬЦЬ КАРЫСТАЛЬНІКАЎ І ДАСТУПНАЯ ПРАПУСКНАЯ ЗДОЛЬНАСЬЦЬ

Правайдэру абыходу трэба вызначыць колькасьць карыстальнікаў і суаднесьці яе з прапускной здольнасьцю канала. Карыстальнік павінен таксама ўлічваць прапускную здольнасьць інтэрнэт-канала, паколькі выкарыстаньне тэхналёгій абыходу запаволіць хуткасьць працы інтэрнэту.

Людзям, якія зьбіраюцца стварыць агульнадаступны проксі-сэрвэр, трэба ўлічваць, што іх сэрвэрам могуць пачаць карыстацца людзі, якія не жывуць у краінах, дзе блякуецца зьмесьціва інтэрнэту. Напрыклад, сэрвэр могуць выкарыстоўваць, каб загружаць цэлыя фільмы, што пагоршыць прапускную здольнасьць канала. З гэтай нагоды вы, магчыма, захочаце абмежаваць доступ да сэрвэра ці трафік. Розныя тэхналёгіі прапануюць некаторыя ці ўсе магчымасьці для вырашэньня гэтай праблемы.

АСНОЎНЫ ПУНКТ ДОСТУПУ І ВЫКАРЫСТАНЬНЕ

У залежнасьці ад месца, зь якога карыстальнік падключаецца да інтэрнэту, і якія паслугі яму патрэбныя ад сістэмы абыходу, існуюць розныя варыянты тэхналёгій абыходу. Напрыклад, карыстальнікі, якія падключаюцца да інтэрнэту з кампутараў грамадзкага карыстаньня ці ў інтэрнэт-кавярнях, ня маюць магчымасьці ўсталяваць праграмнае забесьпячэньне, ім давядзецца выбіраць з варыянтаў, якія прапануе сеціва. Іншыя, магчыма, захочуць выкарыстоўваць ня толькі варыянты ўэб-пошуку (HTTP), але і такія, як электронная пошта (SMTP) ці праграмы перадачы файлаў (FTP). У такім выпадку ім трэба будзе ўсталяваць новае праграмнае забесьпячэньне і зьмяніць устаноўкі кампутара. Безумоўна, для гэтага патрэбныя пэўныя тэхнічныя навыкі.

УЗРОВЕНЬ ТЭХНІЧНАЙ ПАДРЫХТОЎКІ

Чым вышэйшы ўзровень тэхнічнай падрыхтоўкі карыстальніка (і чым менш карыстальнікаў), тым большыя магчымасьці абыходу. Асноўныя праблемы на шляху тэхнічна не падрыхтаваных карыстальнікаў – гэта інсталяцыя і запуск праграм, а таксама любыя зьмены канфігурацыі ці дадатковыя дзеяньні, што выконваюцца ў працэсе выкарыстаньня тэхналёгіі абыходу. Гэта тычыцца як правайдэра абыходу, так і карыстальніка. Няправільнае выкарыстаньне тэхналёгій абыходу для іх можа быць рызыкоўным, але пры правільным выкарыстаньні гэтай рызыкі можна пазьбегнуць.

НАДЗЕЙНЫЯ КАНТАКТЫ

Магчымасьці абыходу павялічваюцца, калі ў карыстальнікаў ёсьць людзі па-за межамі іх краіны, якім яны давяраюць. Калі карыстальнік ня мае надзейных кантактаў, яго магчымасьці зводзяцца да агульнадаступных сыстэмаў, а калі карыстальнік можа знайсьці гэтыя сыстэмы, тое ж самае могуць зрабіць і тыя, хто ажыцьцяўляе фільтрацыю і блякаваньне. Карыстальнік, які мае надзейнага правайдэра абыходу, можа не баяцца, што яго

адсочаць. Яны разам выбіраюць аптымальны для абодвух бакоў варыянт. Пасьпяховае доўгатэрміновае і надзейнае выкарыстаньне тэхналёгій абыходу ў вялікай ступені залежыць ад надзейных кантактаў зь людзьмі, якія жывуць у краінах, дзе фільтрацыя не ажыцьцяўляецца.

МАГЧЫМЫЯ ПАКАРАНЬНІ

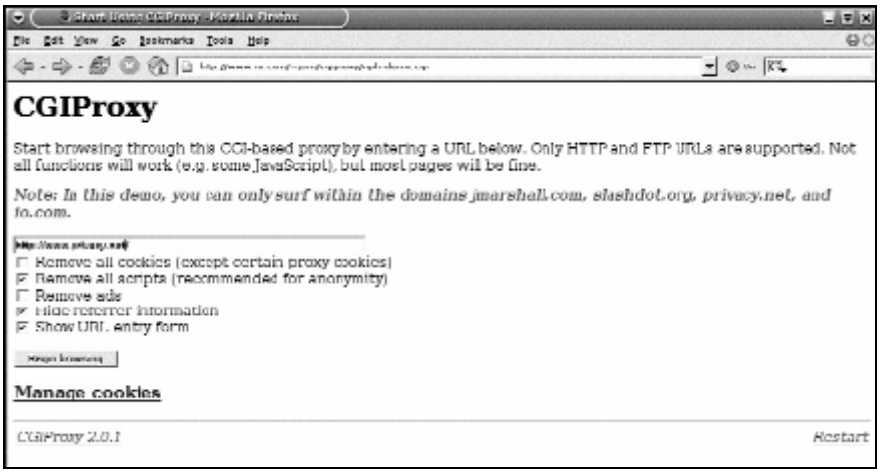
Вельмі важна ведаць, якое пакараньне пагражае карыстальніку тэхналёгій абыходу. У залежнасьці ад суровасьці пакараньня можна выбіраць варыянты тэхналёгій. Калі законы даволя мяккія, і магчымае пакараньне ня надта суровае, карыстальнікі могуць спыніць свой выбар на адным з мноства варыянтаў з даволі высокай эфэктыўнасьцю абыходу, але ня вельмі бясьпечных. Калі ж асяродак небясьпечны, трэба вельмі асьцярожна выбіраць тэхналёгіі з максымальным узроўнем бясьпекі. Магчыма, давядзецца нават прыдумаць легальнае прыкрыцьцё для тэхналёгіі абыходу ці замаскаваць яе неяк па-іншаму.

ПАГРОЗА БЯСЬПЕЦЫ

Даволі часта карыстальнікам прапануюць нейкія тэхналёгіі абыходу, не інфармуючы пры гэтым пра патэнцыйную пагрозу бясьпецы, якую, аднак, можна зьвесьці да мінімуму, калі выбраць правільную тэхналёгію ў правільным месцы і правільна яе выкарыстоўваць.

УЭБ-ТЭХНАЛЁГІІ АБЫХОДУ

Уэб-тэхналёгіі абыходу – гэта спэцыяльныя ўэб-старонкі, дзе ёсьць форма, куды можна проста ўвесьці URL, пасьля чаго онлайнавая сыстэма абыходу знаходзіць патрэбную старонкуі паказвае яе карыстальніку. Паміж карыстальнікам і сайтам, на які ён зрабіў запыт, сувязі няма; сэрвэр, які забясьпечвае абыход, перадае запыт, што дазваляе карыстальніку праглядаць заблякаваныя сайты, застаючыся незаўважаным. Онлайнавыя сэрвэры таксама перапісваюць спасылкі ў старонцы, на якую робіцца запыт, каб карыстальнік мог працягваць інтэрнэт-пошук як звычайна. Каб карыстацца онлайнавымі сыстэмамі абыходу, карыстальніку не трэба ўсталёўваць ніякага дадатковага праграмнага забесьпячэньня ці зьмяняць парамэтры браўзэра. Усё, што трэба - гэта зайсьці на адпаведны сайт, увесьці ў форму URL сайта, які карыстальнік хоча наведаць, і націснуць на "submit". (Сайты онлайнавых праграм абыходу могуць выглядаць па-рознаму, але ўсе яны маюць аднолькавыя базавыя функцыі). Такім чынам, вам ня трэба валодаць нейкімі спэцыяльнымі тэхнічнымі ведамі, каб выкарыстоўваць онлайнавыя праграмы абыходу; акрамя таго, вы можаце імі карыстацца зь любога кампутара.



Proxy-сэрверы / устаноўкі

Перавагі:

Сыстэмы абыходу, даступныя праз інтэрнэт, простыя ў выкарыстаньні і не патрабуюць ад карыстальніка ўсталяваньня дадатковага праграмнага забесьпячэньня.

Карыстальнікі, якія ня маюць надзейных кантактаў па-за межамі краіны, у якой ажыцьцяўляецца фільтрацыя, могуць выкарыстоўваць онлайнавыя праграмы абыходу з кампутараў грамадзкага карыстаньня.

Прыватныя сыстэмы абыходу, даступныя праз інтэрнэт, можна адаптаваць да спэцыфічных патрэб карыстальніка; такія сыстэмы цяжэй адсачыць тым, хто ажыцьцяўляе фільтрацыю.

Недахопы:

Часта онлайнавыя сыстэмы абыходу абмежаваныя ўэб-трафікам (HTTP) і могуць быць закрытыя для шыфраванага доступу (SSL). Уэб-паслугі, якія патрабуюць ідэнтыфікацыі (напрыклад, уэб-пошта) могуць кепска працаваць.

Агульнадаступныя онлайнавыя паслугі абыходу звычайна добра вядомыя і, магчыма, ужо заблякаваныя. Большасьць такіх паслуг ужо заблякаваныя камэрцыйнымі праграмамі фільтрацыі.

Для таго, каб карыстацца прыватнымі онлайнавымі сыстэмамі абыходу, неабходна мець надзейны кантакт у краіне, дзе фільтрацыя не ажыцьцяўляецца. У ідэале трэба, каб абодва бакі (правайдэр і карыстальнік) маглі камунікаваць так, каб іх камунікацыю было вельмі цяжка адсачыць.

АГУЛЬНАДАСТУПНЫЯ ОНЛАЙНАВЫЯ ПАСЛУГІ

Існуе як агульнадаступнае онлайнавае праграмнае забесьпячэньне, так і паслугі. Большасьць такіх паслуг – бясплатныя, але ёсьць і дадатковыя паслугі, якія патрабуюць платнай падпіскі, напрыклад, такія, як шыфраваны доступ. Адныя паслугі прапануюцца кампаніямі, іншыя – па асабістай ініцыятыве для грамадзкага карыстаньня. Вось адрасы некаторых сайтаў, на якіх можна атрымаць такія паслугі:

http://www.anonymizer.com/	http://www.guardster.com/
http://www.unipeak.com/	http://www.webwarper.net/
http://www.anonymouse.ws/	http://www.proximal.com/
http://www.proxyweb.net/	http://www.the-cloak.com/

Паколькі гэтыя адрасы шырока вядомыя, большасьць онлайнавых праграм фільтацыі ўжо маюць іх у сваіх сьпісах - гэта адбываецца ў шмат якіх краінах, дзе фільтрацыя ажыцьцяўляецца на нацыянальным узроўні. Калі гэтыя сайты заблякаваныя, немагчыма атрымаць паслугі, якія яна прапануюць. Акрамя таго, многія агульнадаступныя онлайнавыя паслугі абыходу не прадугледжваюць шыфраваньне трафіку паміж сыстэмай абыходу і карыстальнікам. Любая інфармацыя, адпраўленая карыстальнікам, можа быць перахопленая апэратарам паслуг абыходу.

Агульнадаступныя онлайнавыя праграмы абыходу найбольш падыходзяць карыстальнікам, якія:

- *жывуць у краінах, дзе не існуе сур'ёзнай пагрозы іх бясьпецы;*
- *ня маюць надзейных кантактаў у краінах, дзе фільтрацыя не ажыцьцяўляецца;*
- *маюць сталую ці часовую патрэбу ў паслугах абыходу фільтрацыі;*
- *не перадаюць сакрэтную інфармацыю.*

ПРАГРАМНАЕ ЗАБЕСЬПЯЧЭНЬНЕ ДЛЯ АБЫХОДУ ФІЛЬТРАЦЫІ, ДАСТУПНАЕ ПРАЗЬ СЕЦІВА

Для ўсталяваньня праграмнага забесьпячэньня для абыходу фільтрацыі, даступнага зь сеціва, патрэбная пэўная тэхнічная падрыхтоўка, а таксама рэсурсы (уэб-сэрвэр і прапускная здольнасьць). Пры карыстаньні прыватнымі паслугамі абыходу фільтрацыі месцазнаходжаньне сэрвэра вядомае толькі карыстальніку і правайдэру, у той час як адрасы агульнадаступных сыстэм абыходу і ананімных сэрвэраў вядомыя ня толькі правайдэру і карыстальніку, але і тым, хто ажыцьцяўляе фільтрацыю (гэтая інфармацыя

таксама ёсьць і ў большасьці камэрцыйных сьпісаў фільтрацыі, у адпаведнасьці зь якімі гэтыя сайты блякуюцца). Верагоднасьць выяўленьня і блякіроўкі прыватнай сыстэмы абыходу нашмат меншая, чым агульнадаступнай.

Прыватныя сыстэмы абыходу можна адаптаваць да спэцыфічных патрэбаў карыстальніка. Напрыклад, можна зьмяніць нумар порта на сэрвэры і выканаць шыфраваньне. Пратакол абароненых сокетаў (Secure Socket Layer - SSL) – гэта пратакол, які гарантуе надзейную перадачу дадзеных па сеціве. Ён часта выкарыстоўваецца ўэб-сайтамі ў мэтах канфідэнцыйнай перадачы інфармацыі, напрыклад, калі перадаецца нумар крэдытнай карткі. Доступ да сайтаў, абароненых SSL, забясьпечваецца праз пратакол "HTTPS" замест звычайнага "HTTP".

Наступны варыянт выкарыстаньня SSL – стварыць у корані сэрвэра бяскрыўдную ўэб-старонку і схаваць сыстэму абыходу з дапамогай выбранага наўзгад шляху і імені файла. Нягледзячы на тое, што пасярэднік можа вызначыць, да якога сэрвэра падключаецца карыстальнік, ён ня зможа адсачыць шлях запыту, таму што гэтая частка запыту зашыфраваная. Напрыклад, калі карыстальнік падключаецца да http://example.com/secretcircumventor/, пасярэднік вырашыць, што карыстальнік падключыўся да example.com, але ён ня будзе ведаць, што карыстальнік зьвярнуўся да сыстэмы абыходу. Калі апэратар сыстэмы абыходу разьмесьціць бяскрыўдную старонку на example.com, то сыстэму абыходу нельга будзе знайсьці.

- CGIProxy: CGI скрыпт, працуе як HTTP ці FTP проксі

  http://www.jmarshall.com/tools/cgiproxy
- Peacefire's Circumventor: аўтаматычны інсталятар праграм, з дапамогай якога карыстальнікі, што ня маюць тэхнічнай падрыхтоўкі, змогуць нашмат лягчэй усталяваць і настроіць CGIProxy.

  http://www.peacefire.org/circumventor/simple-circumventor-instructions.html
- pHproxy: экспэрымэнтальная онлайнавая сыстэма абыходу з гнуткай настройкай

  http://ice.citizenlab.org/projects/phproxy
- Psiphon: SSL уэб-сэрвэр з убудаванай онлайнавай сыстэмай абыходу

  http://psiphon.civisec.org

Прыватныя онлайнавыя сыстэмы абыходу з магчымасьцю шыфраваньня лепей за ўсё выкарыстоўваць тым, хто:

- *мае сталую патрэбу ў паслугах абыходу фільтрацыі для працы ў інтэрнэце;*
- *мае надзейныя кантакты ў краінах, дзе зьмесьціва інтэрнэту не фільтруецца;*
- *валодае неабыходнымі тэхнічнымі навыкамі і рэсурсамі, каб запусьціць онлайнавую сыстэму абыходу і падтрымліваць яе функцыі.*

Гэта найбольш гнуткае рашэньне для звычайнага ўэб-трафіку. Такія сыстэмы дастаткова надзейная і добра абароненыя ад блякіроўкі.

ОНЛАЙНАВЫЯ СЫСТЭМЫ АБЫХОДУ: ПЫТАНЬНІ БЯСЬПЕКІ

Сыстэмы абыходу не заўсёды забясьпечваюць ананімнасьць. Праўда, асоба карыстальніка невядомая апэратарам уэб-сайтаў, на якія ён заходзіць. Калі сэанс сувязі паміж карыстальнікам і онлайнавай сыстэмай абыходу праходзіць у звычайным тэкставым рэжыме (HTTP), як у выпадку большасьці бясплатных паслугаў, пасярэднік, такі, як, напрыклад, правайдэр інтэрнэт паслуг (ISP) можа зь лёгкасьцю перахапіць і прааналізавць зьмесьціва. Такім чынам, нават пры пасьпяховым абыходзе фільтрацыі ўлады ўсё роўна могуць даведацца, што карыстальнік выкарыстоўваў онлайнавую сыстэму абыходу. Больш

таго, яны могуць выявіць, якія ўэб-сайты наведаў карыстальнік і якой інфармацыяй абменьваліся онлайнавая сыстэма абыходу і карыстальнік.

Онлайнавыя сыстэмы абыходу, што працуюць у звычайным тэкставым рэжыме (не шыфраваным), час ад часу выкарыстоўваюць замену знакаў URL, каб заблытаць праграмы фільтрацыі зьмесьціва па ключавых словах у URL (Uniform Resource Locator). Напрыклад, выкарыстаньне простай тэхнікі, такой, як ROT-13, дзе нейкая літара замяняецца на іншую, якая ў алфавіце стаіць на трынаццаць літар раней за яе. Напрыклад, наступны URL: http://ice.citizenlab.org пераўтвараецца ў uggc://vpgvmrayno.bet. Па сутнасьці, тэкст URL кадуецца такім чынам, каб ключавых словаў, па якіх ажыцьцяўляецца фільтрацыя, не было ў дадзеным URL. Тым ня менш, зьмесьціва, з якім працаваў карыстальнік падчас сэансу сувязі, можна адсачыць нават у выпадку ўдалага абыходу.

Таксама існуе рызыка, зьвязаная з выкарыстаньнем "scripts"і "cookies"(фрагмэнты дадзеных пра папярэднія запыты карыстальнікаў). Шмат якія онлайнавыя сыстэмы абыходу можна настроіць так, каб яны выдалялі "cookies" і "scripts", аднак многія сайты (напрыклад, сайты ўэб-пошты) патрабуюць ад карыстальнікаў іх прымаць. Пры актывізацыі опцый выдаленьня "scripts" і "cookies" трэба быць вельмі асьцярожным. Рызыка ёсьць і ў выпадку сувязі з сыстэмай абыходу ў звычайным тэкставым фармаце з далейшым яе выкарыстаньнем для запыту інфармацыі з шыфраванага сэрвэра, асабліва пры карыстаньні паслугамі, для атрыманьня якіх трэба ўводзіць пароль. У гэтым выпадку сыстэма абыходу атрымлівае інфармацыю, на якую быў дасланы запыт, з SSLсэрвэра ў зашыфраваным выглядзе, але потым дасылае зьмесьціва карыстальніку ў звычайным тэкставым фармаце. Такім чынам, сакрэтная інфармацыя можа быць перахопленая.

Некторыя зь пералічаных праблем зь бясьпекай можна вырашыць, усталяваўшы шыфраваную сувязь з онлайнавымі проксі-сэрвэрамі. Доступ да некаторых онлайнавых проксі-сэрвэраў магчымы праз SSL (HTTPS), які шыфруе сувязь паміж карыстальнікам і онлайнавай сыстэмай абыходу. У гэтым выпадку пасярэднікі могуць даведацца толькі пра тое, што карыстальнік падключыўся да онлайнавай сыстэмы абыходу, але яны не атрымаюць доступ да зьмесьціва. Настойліва раю карыстальнікам, каб выкарыстоўвалі онлайнавыя SSL сыстэмы абыходу, калі існуе высокая пагроза бясьпецы.

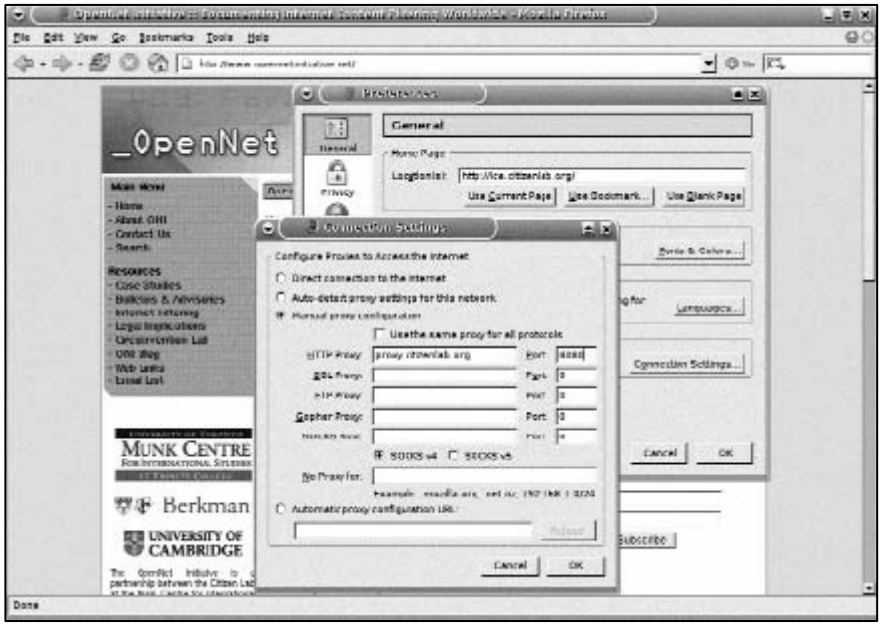
Аднак нават калі сувязь карыстальніка з онлайнавай сыстэмай абыходу надзейна абароненая, уладальнік онлайнавай сыстэмы абыходу можа перахапіць любую інфармацыю, што праходзіць праз сыстэму. Інфармацыя, якую захоўвае правайдэр паслуг абыходу - таксама пагроза бясьпецы. У залежнасьці ад месцазнахожданьня сыстэмы абыходу ці сэрвэра ўлады могуць мець доступ да рэгістрацыйных запісаў сыстэмы (log files).

Карыстальнікі павінныя разумець, што і пры выкарыстаньні онлайнавых SSL сыстэм абыходу існуе пэўная небясьпека. Напрыкалад, шыфраваньне, якое не паўсюль ухваляецца законам, можа прыцягнуць дадатковую ўвагу да працы карыстальніка з онлайнавымі сыстэмамі абыходу. Таксама структуры, якія ажыцьцяўляюць фільтрацыю, могуць вызначыць, на якія сайты заходзіць карыстальнік з дапамогай онлайнавых сыстэм абыходу, нават калі ён выкарыстоўвае SSL тэхнікі з элементамі шыфраваньня, такія, як атакі HTTP fingerprinting і Man-In-The-Middle (MITM). Тым ня менш, старонкі з дынамічным зьмесьцівам ці сыстэмы абыходу, якія дадаюць да зьмесьціва, на якое быў дасланы запыт, фальшывыя тэксты ці выявы ў адвольных колькасьцях, могуць значна зьнізіць ступень рызыкі. Калі карыстальнік мае "адбіткі пальцаў" ("fingerpritnt") ці лічбавы подпіс SSL сэртыфіката, ён можа ўручную праверыць аўтэнтычнасьць сэртыфіката, пазьбягаючы MITM атакі[1].

ПРОКСІ-СЭРВЭРЫ

[1] Больш падрабязна пра магчымыя атакі на сыстэмы абыходу можна даведацца з артыкула Бенета Хэйзэлтана (Bennett Haselton) "Сьпіс магчымых слабых месцаў сыстэм абыходу інтрэнэт-цэнзуры" ("List of possible weaknesses in systems to circumvent Internet censorship") на http://peacefire.org/circumventor/list-of-possible-weaknesses.html, а таксама з адказу Паўла Бараноўскага (Paul Baranowski) на http://www.peek-a-booty.org/pbhtml/downloads/ResponseToLopwistcic.pdf

Проксі-сэрвэр – гэта сэрвэр, які знаходзіцца паміж кліентам (такім, як уэб-браўзэр) і сэрвэрам (такім, як уэб-сэрвэр). Проксі-сэрвэр дзейнічае як буфэр паміж кліентам і сэрвэрам і можа падтрымліваць мноства розных запытаў дадзеных, у тым ліку ўэб-трафік (HTTP), перадачу файлаў (FTP) і шыфраваны трафік (SSL). Проксі-сэрвэры выкарыстоўваюцца прыватнымі асобамі, арганізацыямі і краінамі ў розных мэтах, у тым ліку, для забесьпячэньня бясьпекі, ананімнасьці, кэшаваньня і фільтрацыі. Для таго, каб пачаць карыстацца проксі-сэрвэрам, карыстальніку неабходна настроіць парамэтры свайго ўэб-браўзэра ў адпаведнасьці з IP адрасам ці імем хоста проксі-сэрвэра, а таксама з нумарам порта, які выкарыстоўвае проксі-сэрвэр. Хоць гэта і не складаная праца, але правесьці яе на кампутарах грамадзкага карыстаньня (зьмяніць парамэтры браўзэра), напрыклад, у біблятэцы, інтэрнэт-кавярні ці на працы, можа аказацца немагчымым.



Перавагі:

Існуе вялікі выбар праграмных пакетаў, якія дазваляюць празрыста выкарыстоўваць розныя тыпы трафіку, а ня толькі ўэб-трафік (HTTP), і якія можна настроіць для работы на нестандартных портах. Ёсьць шмат агульнадаступных проксі-сэрвэраў.

Недахопы:

Шмат якія проксі-сэрвэры не выконваюць шыфраваньне па змоўчаньні, таму трафік паміж карыстальнікам і сэрвэрам нельга назваць надзейным.

Карыстальніку трэба атрымаць дазвол на зьмену настройкі парамэтраў браўзэра, і калі правайдэр інтрэнэт паслуг патрабуе, каб трафік праходзіў празь яго проксі-сэрвэр, выкарыстоўваць агульнадаступны проксі-сэрвэр будзе немагчыма.

Калі закон не дазваляе выкарыстаньне агульнадаступных проксі-сэрвэраў, то яны не заўсёды будуць даступныя для карыстальніка.

ПРАГРАМНАЕ ЗАБЕСЬПЯЧЭНЬНЕ ПРОКСІ-СЭРВЭРАЎ

Праграмнае забесьпячэньне проксі-сэрвэраў можа быць усталяванае надзейнымі людзьмі ў краінах, дзе зьмесьціва інтэрнэту не фільтруецца. Гэтыя людзі павінныя мець пэўныя тэхнічныя веды. Праграмнае забесьпячэньне проксі-сэрвэраў трэба ўсталёўваць там, дзе магчымая вялікая прапускная здольнасьць інтэрнэт-канала. Акрамя таго, неабходна выкарыстоўваць тэхналёгію крыптаграфіі. Гэты варыянт найбольш зручны ў сытуацыі, калі, напрыклад, фірма ці невялікая арганізацыя маюць сталую патрэбу ў выкарыстаньні сыстэмы абыходу. Пасьля таго, як карыстальнік у краіне, дзе зьмесьціва інтэрнэту фільтруецца, настроіць свой браўзэр для работы праз проксі-сэрвэр, ён можа празрыста працаваць у інтэрнэце. Нягледзячы на тое, што выкарыстаньне прыватнага проксі-сэрвэра не забясьпечвае ананімнасьць на сто адсоткаў, гэта лепшае рашэньне, чым выкарыстаньне онлайнавых проксі-сыстэм, напрыклад, для доступу да сайтаў, якія патрабуюць ідэнтыфікацыі і абавязковага прыёму “cookies”, напрыклад, сайтаў уэб-пошты. Проксі-сэрвэры можна таксама адаптаваць да спэцыфічных патрэбаў карыстальніка і да мясцовых мэханізмаў фільтрацыі.

- Squid – гэта бясплатнае праграмнае забесьпячэньне проксі-сэрвэра, узмацніць абарону якога можна з дапамогай сэрвэра Stunnel.

http://www.squid-cache.org, http://www.stunnel.org, http://ice.citizenlab.org/projects/aardvark

- Privoxy – гэта проксі-сэрвэр з дадатковымі магчымасьцямі для абыходу фільтрацыі
- http://www.privoxy.org
- Secure Shell (SSH) мае ўбудаваны socks proxy ($ssh-D port secure.host.com)
- http://www.openssh.com
- HTTPport/HTTPhost дазваляе абыйсьці ваш HTTP проксі-сэрвэр, якія блякуе вам доступ да інтэрнэту.

Прыватныя проксі-сэрвэры з магчымасьцю шыфраваньня лепей за ўсё выкарыстоўваць фірмам ці арганізацыям, якія маюць сталую патрэбу ў выкарыстаньні сыстэм абоду фільтрацыі. Такі сэрвэр павінен знаходзіцца па-за межамі краіны, забясьпечваць неабыходную прапускную здольнасьць і падтрымлівацца надзейнымі людзьмі, якія валодаюць неабыходнымі тэхнічнымі ведамі.

АГУЛЬНАДАСТУПНЫЯ ПРОКСІ-СЭРВЭРЫ

Адкрытыя проксі-сэрвэры – гэта сэрвэры, якія наўмысна ці зь іншай нагоды адкрытыя для сувязі з аддаленымі кампутарамі. Дакладана невядома, ці адкрытыя проксі-сэрвэры першапачаткова былі створаныя з мэтай адкрытага доступу, ці так атрымалася ў выніку няправільнай настройкі парамэтраў.

УВАГА: У некаторых краінах закон можа трактаваць выкарыстаньне проксі-сэрвэраў як “несанкцыянаваны доступ”, а іх карыстальнікам можа пагражаць пакараньне. Таму выкарыстаньне адкрытых проксі-сэрвэраў не рэкамэндуецца.

Месцазнаходжаньне адкрытых проксі-сэрвэраў

Шмат якія ўэб-сайты прапануюць сьпісы адкрытых проксі-сэрвэраў, аднак, няма гарантыі, што пералічаныя ў сьпісах сэрвэры дагэтуль дзейнічаюць. Таксама не гарантуецца дакладнасьць інфармацыі, асабліва ў дачыненьні да ступені ананімнасьці і геаграфічнага распалажэньня проксі-сэрвэраў. Памятайце, што вы карыстаецеся гэтымі сэрвэрамі на сваю рызыку.

Уэб-сайты са сьпісамі адкрытых проксі-сэрвэраў:

http://www.samair.ru/proxy/

http://www.antiproxy.com/

http://tools.rosinstrument.com/proxy/

http://www.multiproxy.org/

http://www.publicproxyservers.com/

Праграмнае забесьпячэньне: ProxyTools/LocalProxy

http://proxytools.sourceforge.net

Адкрытыя проксі-сэрвэры: нестандартныя порты

У некаторых краінах, дзе фільтрацыя ажыцьцяўляецца на нацыянальным узроўні, блякуецца доступ да стандартных проксі-портаў. "Порт" – гэта абстрактны панятак, які выкарыстоўваецца транспартным пратаколам інтэрнэту для абазначэньня злучэньня. Пры розных інтэрнэт паслугах дадзеныя перадаюцца праз пэўныя нумары портаў. Канкрэтныя пратаколы і сэрвісы атрымліваюць нумары портаў праз структуру "Цэнтральны каардынытыр па прысваеньні ўнікальных парамэтраў інітэрнэт пратаколаў" ("Internet Assigned Numbers Authority" (IANA). Напрыклад, порт 80 зарэзарваваны для HTTP трафіка. Калі браўзэр атрымлівае доступ да нейкага сайта, насамрэч усталёўваецца сувязь з уэб-сэрвэрам, які працуе праз порт 80. Проксі-сэрвэры таксама маюць порты, якія аўтаматычна ім прысвойваюцца. Таму шмат якія тэхналёгіі фільтрацыі блякуюць доступ да гэтых портаў. Каб пасьпяхова абыйсьці фільтрацыю, неабходна выкарыстоўваць проксі-сэрвэр, настроены на работу праз нестандартны порт.

http://www.web.freerk.com/proxylist.htm

ПРОКСІ-СЭРВЭРЫ: ПЫТАНЬНІ БЯСЬПЕКІ

Канфігурацыя проксі-сэрвэраў мае вельмі вялікае значэньне, таму што ад яе залежыць бясьпека і ананімнасьць сувязі. Акрамя таго, што проксі-сэрвэры не забясьпечваюць шыфраваньне дадзеных, яны могуць перадаваць інфармацыю пра карыстальніка на сэрвэр, які атрымаў запыт на зьмесьціва. Гэта дае магчымасьць вызначыць IP адрас кампутара, зь якога быў атрыманы запыт. А паколькі сувязь паміж вамі і проксі-сэрвэрам ажыцьцяўлецца ў рэжыме адкрытага тэксту, структурам, што фільтруюць зьмесьціва, лёгка яго перахапіць. Больш таго, любая інфармацыя, што праходзіць праз проксі-сэрвэр, можа быць перахопленая яго ўладальнікам.

Таму я ня раю займацца пошукам агульнадаступных проксі-сэрвэраў і іх выкарыстоўваць. Адкрытыя проксі-сэрвэры часта выкарыстоўваюцца з нагоды даступнасьці, але яны не зьяўляюцца бясьпечнымі, хоць і дазваляюць пасьпяхова абыйсьці фільтрацыю.

Як і онлайнавыя проксі, проксі-сэрверы маюць тыя ж праблемы зь бясьпекай. Карыстальніку будуць дасылацца шкодныя "scripts" і "cookies". Акрамя таго, нават пры выкарыстаньні інструмэнтаў шыфраваньня проксі-сэрвэры адкрытыя для атак ("fingerprinting attacks") MITM і HTTP. Трэба ўлічваць і тое, што пры выкарыстаньні некаторых браўзэраў магчымая ўцечка інфармацыі пры злучэньні з проксі-сэрвэрамі, якія забясьпечваюць не толькі ўэб-трафік, але і іншыя віды трафіку ("socks proxies"). Калі робіцца запыт на нейкі ўэб-сайт, назва дамэну пераўтвараецца ў IP адрас. Некаторыя браўзэры выконваюць гэтую апэрацыю самі, г.зн. працэс праходзіць без удзелу проксі. У такіх выпадках запыт пра IP адрас заблякаванага сайта робяць сэрвэры "Сыстэмы назваў дамэнаў" ("Domain Name System" (DNS)) у краінах, дзе ажыцьцяўляецца фільтрацыя[2].

Я ня раю выкарыстоўваць адкрытыя проксі-сэрвэры. Такія сэрвэры прыдатныя ў выпадках, калі патрэба ў іх выкарыстаньні мае часовы ці пэрыядычны характар у краінах, і дзе выкарыстаньне проксі-сэрвэраў не зьвязанае з сур'ёзнай рызыкай. Агульнадаступныя проксі-сэрвэры ня варта выкарыстоўваць для перадачы канфідэнцыйнай інфармацыі.

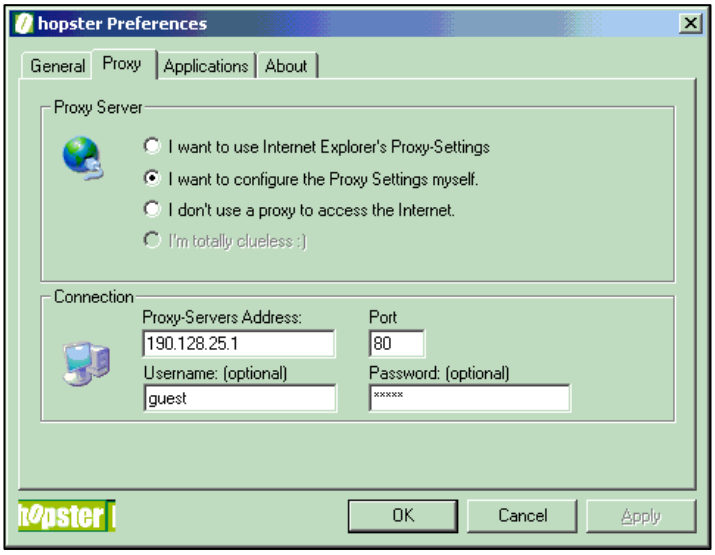
---

[2] Болей інфармацыі на сайце: http://tor.eff.org/cvs/tor/doc/CLIENTS

ТУНЭЛЯВАНЬНЕ

Тунэляваньне, ці пераадрасацыя портаў, дазваляе схаваць неабаронены нешыфраваны трафік у зашыфраваным пратаколе. Карыстальнік у краіне, дзе ажыцьцяўляецца фільтрацыя, загружае кліенцкую праграму, якая стварае тунэль да кампутара, які знаходзіцца па-за межамі зоны фільтрацыі. Карыстальнік мае доступ да звычайных сэрвісаў, аднак яны ідуць праз шыфраваны тунэль да кампутара, што знаходзіцца ў бясьпечным месцы. Гэты кампутар, у сваю чаргу, празрыста накіроўвае запыты і адказы карыстальнікаў. Існуе шмат праграм для тунэляваньня. Карыстальнікі, якія маюць кантакты ў краінах, дзе няма фільтрацыі інтэрнэту, могуць карыстацца прыватнымі паслугамі тунэляваньня. Тыя ж, хто ня мае такіх кантактаў, могуць падпісацца на платныя камэрцыйныя паслугі.

Як правіла, пры карыстаньні бясплатнымі паслугамі тунэляваньня даводзіцца лічыцца з рэклямай. Запыты на разьмяшчэньне рэклямы перадаюцца ў звычайным тэкставым рэжыме (HTTP). Гэтыя запыты могуць быць перахопленыя, і пасярэднік зможа даведацца пра карыстаньне паслугамі пераадрасацыі. Больш таго, у многіх паслугах тунэляваньня выкарыстоўваюцца "sock proxies", што можа прывесьці да таго, што стануць вядомыя назвы дамэнаў, на якія робіцца запыт.



http://www.http-tunnel.com/

http://www.hopster.com/

http://www.htthost.com/

Перавагі:

Карыстаньне паслугамі пераадрасацыя портаў забясьпечвае перадачу шыфраваных дадзеных.

Пры карыстаньні пераадрасацыяй портаў выкарыстоўваецца ня толькі ўэб-трафік, але і шмат іншых пратаколаў.

Існуюць камэрцыйныя паслугі, па якія могуць зьвярнуцца карыстальнікі, што ня маюць кантактаў у краінах, дзе зьмесьціва інтэрнэту не фільтруецца.

Недахопы:

Камэрцыйныя паслугі пераадрасацыі портаў агульнавядомыя і, магчыма, ужо фільтруюцца.

Паслугамі тунэляваньня нельга карыстацца ў месцах грамадзкага доступу да інтэрнэту, дзе немагчыма ўсталяваць сваё праграмнае забесьпячэньне, напрыклад, у інтэрнэт-кавярніх і бібліятэках.

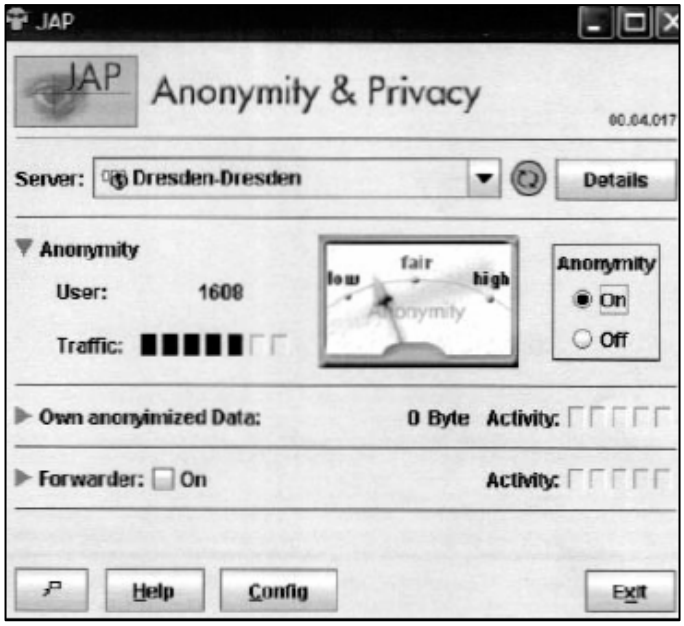
Каб карыстацца паслугамі тунэляваньня, могуць спатрэбіцца больш глыбокія тэхнічныя веды, чым для іншых спосабаў абыходу фільтрацыі.

Тэхналёгіі пераадрасацыі портаў аптымальныя для карыстальнікаў, якія валодаюць пэўнымі тэхнічнымі ведамі, якія маюць патрэбу ў надзейных, а не ананімных паслугах абыходу фільтрацыі ня толькі для ўэб-трафіку. Акрамя таго, яны не карыстаюцца інтэрнэтам у месцах грамадзкага доступу. Камэрцыйныя паслугі тунэляваньня – выдатнае рашэньне праблемы для карыстальнікаў, якія ня маюць надзейных кантактаў у краінах, дзе не ажыцьцяўляецца фільтрацыя.

АНАНІМНЫЯ КАМУНІКАЦЫЙНЫЯ СЫСТЭМЫ

Тэхналёгіі абыходу і ананімныя камунікацыйныя сыстэмы падобныя і часта ўзаемадзейнічаюць, але маюць розныя мэты. Ананімныя камунікацыйныя сыстэмы перш за ўсё забясьпечваюць ананімнасьць карыстальніка, хаваючы яго асобу ад правайдэра зьмесьціва. Акрамя таго, больш дасканалыя сыстэмы выкарыстоўваюць разнастайныя тэхнікі маршрутызацыі, каб схаваць асобу карыстальніка ад самой ананімнай камунікацыйнай сыстэмы. Сыстэмы абыходу не заўсёды забясьпечваюць ананімнасьць. Яны могуць быць накіраваныя на забесьпячэньне надзейнай сувязі, каб абыйсьці нейкія абмежаваньні, з прычыны якіх карыстальнік ня можа адпраўляць і атрымліваць інтэрнэт-паведамленьні. Для таго, каб абыйсьці абмежаваньні зьмесьціва, патрэбная тэхналёгія надзейных камунікацый і часта некаторая "маскіроўка", але не абавязкова ананімнасьць.

Ананімныя камунікацыйныя сыстэмы часта выкарыстоўваюцца для абыходу фільтрацыі. Іх галоўная перавага ў тым, што існуе некалькі сетак, увайшоўшы ў якія можна абыйсьці забароны на доступ да зьмесьціва, захоўваючы ананімнасьць.



Выкарыстаньне ананімных камунікацыйных сыстэм для абыходу фільтрацыі патрабуе кампутара, на якім карыстальнік можа ўсталяваць патрэбнае праграмнае забесьпячэньне. Тыя, хто карыстаецца інтэрнэтам праз адкрытыя (грамадзкія) тэрміналы, у бібліятэках ці інтэрнэт-кавярніях, хутчэй за ўсё, ня змогуць выкарыстоўваць такія сыстэмы для абыходу фільтрацыі. Акрамя таго, ананімныя камунікацыйныя сыстэмы могуць запавольваць хуткасьць інтэрнэт-сувязі.

Карыстальнікі, якія хочуць абыйсьці інтэрнэт-фільтрацыю на дзяржаўным узроўні ці на ўзроўні правайдэра інтэрнэт-паслуг (ISP), могуць сутыкнуцца з тым, што структуры, якія ажыцьцяўляюць фільтрацыю, блякуюць доступ да ананімных камунікацыйных сыстэм. Калі выкарыстоўваецца сыстэма, якая функцыянуе праз статычны порт, праграмы фільтрацыі можна зь лёгкасьцю настроіць на блякаваньне доступу. Чым ананімная камунікацыйная сыстэма больш вядомая, тым большая рызыка, што яна будзе заблякаваная. Акрамя таго, для барацьбы з сыстэмамі, што выкарыстоўваюць аднарангавыя ці агульнадаступныя вузлы, структуры, якія ажыцьцяўляюць фільтрацыю, могуць проста зачыніць доступ гэтым хостам. Структуры, што ажыцьцяўляюць фільтрацыю, могуць запусьціць уласны вузел, каб адсачыць карыстальнікаў, якія будуць спрабаваць да

яго падключыцца. У некаторых краінах, дзе трафік да добра вядомых сыстэмаў адсочваецца, выкарыстаньне гэтых сыстэм можа прыцягнуць увагу да карыстальнікаў[3].

Перавагі:

Яны забясьпечваюць як бясьпеку, так і ананімнасьць.

Яны даюць магчымасьць бясьпечнага доступу з выкарыстаньнем розных пратаколаў, не абмяжоўваючыся ўэб-трафікам.

Існуюць супольнасьці карыстальнікаў гэтых праграм і іх распрацоўшчыкаў, якія могуць аказаць тэхнічную дапамогу.

Недахопы:

Яны ня створаныя спэцыяльна для абыходу. Яны агульнавядомыя, і іх можна лёгка фільтраваць.

Імі нельга карыстацца ў месцах грамадзкага доступу да інтэрнэту, напрыклад, у бібліятэках і інтэрнэт-кавярнях, дзе немагчыма ўсталяваць праграмнае забесьпячэньне.

- **Tor** – гэта сетка віртуальных тунэляў, якая дазваляе індывідуальным карыстальнікам і групам павысіць узровень іх бясьпекі і забясьпечыць ананімнасьць у інтэрнэце. Яна таксама дазваляе распрацоўшчыкам праграмнага забесьпячэньня ствараць новыя інструмэнты камунікацый з убудаванымі функцыямі бясьпекі. Tor забясьпечвае аснову для шэрагу прылажэньняў, якія даюць магчымасьць арганізацыям і асобам абменьвацца інфармацыяй праз адкрытыя (грамадзкія) сеткі, захоўваючы канфідэнцыйнасьць.

  http://tor.eff.org

- **JAP** дазваляе ажыцьцяўляць інтэрнэт-пошук ананімна. Замест наўпроставага падключэньня да ўэб-сэрвэра, карыстальнік ідзе ў абыход, выкарыстоўваючы шыфраванае падключэньне празь некалькіх пасярэднікаў, такзваных "міксаў" (mixes").

  http://anon.inf.tu-dresden.de/index_en.html

- **Freenet** - гэта бясплатнае праграмнае забесьпячэньне, якое дазваляе разьмяшчаць і атрымліваць інфармацыю ў інтэрнэце, не баючыся цэнзуры. Яно цалкам дэцэнтралізаванае, а ананімнасьць тых, хто разьмяшчае і спажывае інфармацыю, цалакам захоўваецца.

  http://freenet.sourceforge.net

Выкарыстаньне такіх сыстэмаў можа патрабаваць даволі высокага ўзроўню тэхнічнай падрыхтоўкі.

Ананімныя камунікацыйныя сыстэмы разьлічаныя на тэхнічна граматных карыстальнікаў, якія маюць патрэбу ў паслугах як па абыходзе фільтрацыі, так і забесьпячэньні ананімнасьці ня толькі для ўэб-трафіку, але і іншай дзейнасьці. Такімі сыстэмамі нельга карыстацца ў пунктах грамадзкага доступу да інтэрнэту.

ВЫСНОВЫ

[3] Болей інфармацыі пра магчымыя атакі на сыстэмы абыходу можна атрымаць з артыкула Бенета Хэйзэлтана (Bennett Haselton) "Сьпіс магчымых слабых месцаў у сыстэмах абыходу інтэрнэт-цэнзуры" ("List of possible weaknesses in systems to circumvent Internet censorship) на http://peacefire.org/circumventor/list-of-possible-weaknesses.html і адказ Паўла Бараноўскага на www.peek-a-booty.org/pbhtml/downloads/ResponseToLopwistcic.pdf

Рашэньне выкарыстоўваць тэхналёгіі абыходу трэба прымаць, усьведамляючы сур'ёзнасьць такога кроку. Неабходна прааналізаваць канкрэтныя патрэбы і даступныя рэсурсы, а таксама разгледзець пытаньні бясьпекі. Існуе шэраг тэхналёгій, даступных для карыстальнікаў, якія маюць патрэбу ў паслугах абыходу інтэрнэт-фільтрацыі. Аднак іх удалае выкарыстаньне залежыць ад шэрагу фактараў, у тым ліку, ад узроўню тэхнічных ведаў карыстальніка, магчымай пагрозы яга бясьпецы, а таксама ад наяўнасьці (ці адсутнасьці) надзейных кантактаў у краіне, дзе фільтрацыя не ажыцьцяўляецца. Улады, у сваю чаргу, могуць прыймаць контр-меры для эфектыўнага блякаваньня пэўных тэхналёгій абыходу.

Ключы да пасьпяховага і стабільнага выкарыстаньня тэхналёгій абыходу – гэта давер і правільнае выкананьне. Сыстэмы абыходу мусяць быць арыентаваныя на карыстальнікаў у канкрэтных абставінах ці мець магчымасьць адаптацыі да патрэбаў карыстальніка. Ад такіх сыстэмаў патрабуецца надзейнасьць, магчымасьць перанастройкі і часта здольнасьць "замаскавацца". Неабходна, каб правайдэр паслуг абыходу фільтрацыі і карыстальнік давяралі адзін аднаму, яны павінныя ведаць спэцыфіку юрыдычнай і палітычнай сытуацыі карыстальніка, а таксама ўсьведамляць, што тэхналёгій абыходу маюць абмежаваньні.

Нарт Віленёв – кіраўнік тэхнічных дасьледаваньняў "Грамадзянскай лябараторыі" ("The Citizen Lab") – міждысцыплінарнай лябараторыі Цэнтра міжнародных дасьледаваньняў імя Мунка ўва Ўнівэрсітэце Таронта (The Munk Centre for International Studies at the University of Toronto). Ён займаецца як навуковымі дасьледаваньнямі, так і распрацоўкамі праграмнага забесьпячэньня. Цяпер ён супрацоўнічае з арганізацыяй "OpenNet Initiative" (ONI). У рамках гэтага супрацоўніцтва Нарт Віленёв зьбірае інфармацыю пра фільтрацыю і кантроль інтэрнэт-зьмесьціва ў сьвеце. Ён таксама зьбіраў інфармацыю пра існуючыя тэхналёгіі абыходу і рабіў іх ацэнку, а таксама займаўся распрацоўкай тэхналёгій абыходу. Акрамя інтэрнэт-цэнзуры, ён дасьледуе праблемы хактывізму, кібэртэрарызму і інтэрнэт-бясьпекі. Нарт Віленёв нядаўна скончыў навучаньне ва Ўнівэрсітэце Таронта па праграме "Мір і канфлікт".

Нарт Віленёв выказвае ўдзячнасьць Мішэлю Левеску (Michelle Levesque), Дэрэку Бамбаўэру (Derek Bambauer) і Бенету Хэйзэлтану (Bennett Haselton).

ЯК ЗАБЯСЬПЕЧЫЦЬ **КАНФІДЭНЦЫЙНАСЬЦЬ** ЭЛЕКТРОННАГА ЛІСТАВАНЬНЯ

Людовік Пьера (Ludovic Pierrat)

У большасьці краін улады маюць магчымасьці праглядаць электонную пошту. У краінах з рэпрэсіўным рэжымам "кібэрпаліцыя" выкарыстоўвае гэтыя магчымасьці, каб адсочваць і арыштоўваць палітычных апанэнтаў; многія палітычныя лідэры патрапляюць за краты за адпраўленьне, ці нават перасылку электронных паведамленьняў. Адзін палітычны дысыдэнт на Мальдывах быў асуджаны на 15 год турэмнага зьняволеньня за электроннае ліставаньне з праваабарончай арганізацыяй "Amnesty International". Карыстальнік інтэрнэту ў Сырыі зь лютага 2003 году знаходзіцца ў турме за перасылку бюлетэня, што распаўсюджваецца па электроннай пошце.

Такім чынам, я прапаную некаторыя парады, як забясьпечыць канфідэнцыйнасьць электроннай пошты.

Карыстаньне адрасам электроннай пошты, выдадзеным вашым інтэрнэт-правайдэрам (ISP), напрыклад, AOL, Wanadoo ці Free, або адрасам, выдадзеным кампаніяй, у якой вы працуеце, не гарантуе канфідэнцыйнасьці электроннага ліставаньня. Уладальнікі сетак, празь якія праходзяць вашыя паведамленьні, могуць зь лёгкасьцю іх перахопліваць. Калі ўлады ў нейкай краіне пачынаюць сачыць за карыстальнікамі інтэрнэту, то звычайна атрымліваюць доступ да іх электроннай карэспандэнцыі праз правайдэраў.

Адрасы ўэб-пошты, такія, як Yahoo! ці Hotmail, больш надзейныя, таму што тут не выкарыстоўваюцца сэрвэры мясцовых правайдэраў. Каб кантраляваць такое ліставаньне, трэба неяк "прабіцца" ў сыстэму ці перахопліваць пасланьні падчас іх перасылкі, што тэхнічна больш складана. Нажаль, гэтая перавага вельмі адносная, таму што кампутарныя спэцыялісты з паліцыі ці хакеры ўсё адно могуць праглядаць вашую пошту.

Шыфраваньне (абарона пошты з дапамогай коду) – асноўны спосаб рэальна забясьпечыць канфідэнцыйнасьць вашых паведамленьняў. Ёсьць два спосабы шыфраваньня:

КЛЯСЫЧНАЕ ШЫФРАВАНЬНЕ

Эн і Майкл хочуць весьці сакрэтнае ліставаньне. Яны дамаўляюцца пра коды зашыфроўкі і расшыфроўкі, а таксама пра ключ, і пачынаюць ліставаньне.

З гэтым спосабам можа паўстаць праблема, калі трэцяя асоба перахопіць паведамленьне, у якім Эн і Майкл абменьваюцца ключамі. Акрамя таго, што іх ліставаньне будуць чытаць, ім яшчэ могуць дасылаць і фальшывыя паведамленьні. Такім чынам, Эн і Майклу трэба абмяняцца ключамі так, каб ніхто гэтага ня ўбачыў, напрыклад, пры асабістай сустрэчы.

АСЫМЭТРЫЧНАЕ ШЫФРАВАНЬНЕ

Найлепшы спосаб вырашэньня праблемы канфідэнцыйнасьці – гэта "асымэтрычнае" шыфраваньне. Для гэтага патрэбныя два ключы – адзін для зашыфроўкі, другі – для

расшыфроўкі. Ключом для зашыфроўкі ("адкрытым ключом") можна абмяняцца праз інтэрнэт не баючыся, таму што зь яго дапамогай немагчыма расшыфраваць пасланьне. Ключ для расшыфроўкі ("сакрэтны" ці "закрыты" ключ) не абмяркоўваецца.

Пры асымэтрычным шыфраваньні Эн мае два ключы (адкыты, які яна паведамляе, і закрыты, якога ніхто ня ведае). Эн дасылае свой ключ Майклу. З дапамогай гэтага ключа Майкл зашыфроўвае свае пасланьні да Эн. Толькі Эн з дапамогай свайго сакрэтнага ключа можа расшыфраваць пасланьні Майкла. Майкл мае свае два ключы. Ён, у сваю чаргу, дасылае Эн свой адкрыты ключ. Такім чынам, Эн адказвае на пасланьні Майкла, не турбуючыся пра канфідэнцыйнасьць паведамленьняў.

Але паколькі адкрыты ключ перадаецца праз інтэрнэт без нейкай спэцыяльнай абароны, лепей разам зь яго аўтарам яго ўзгадніць. Кожны ключ мае "адбіткі пальцаў" (кароткі набор сымбаляў, знакаў), якія можна перадаць асабіста ці па тэлефоне.

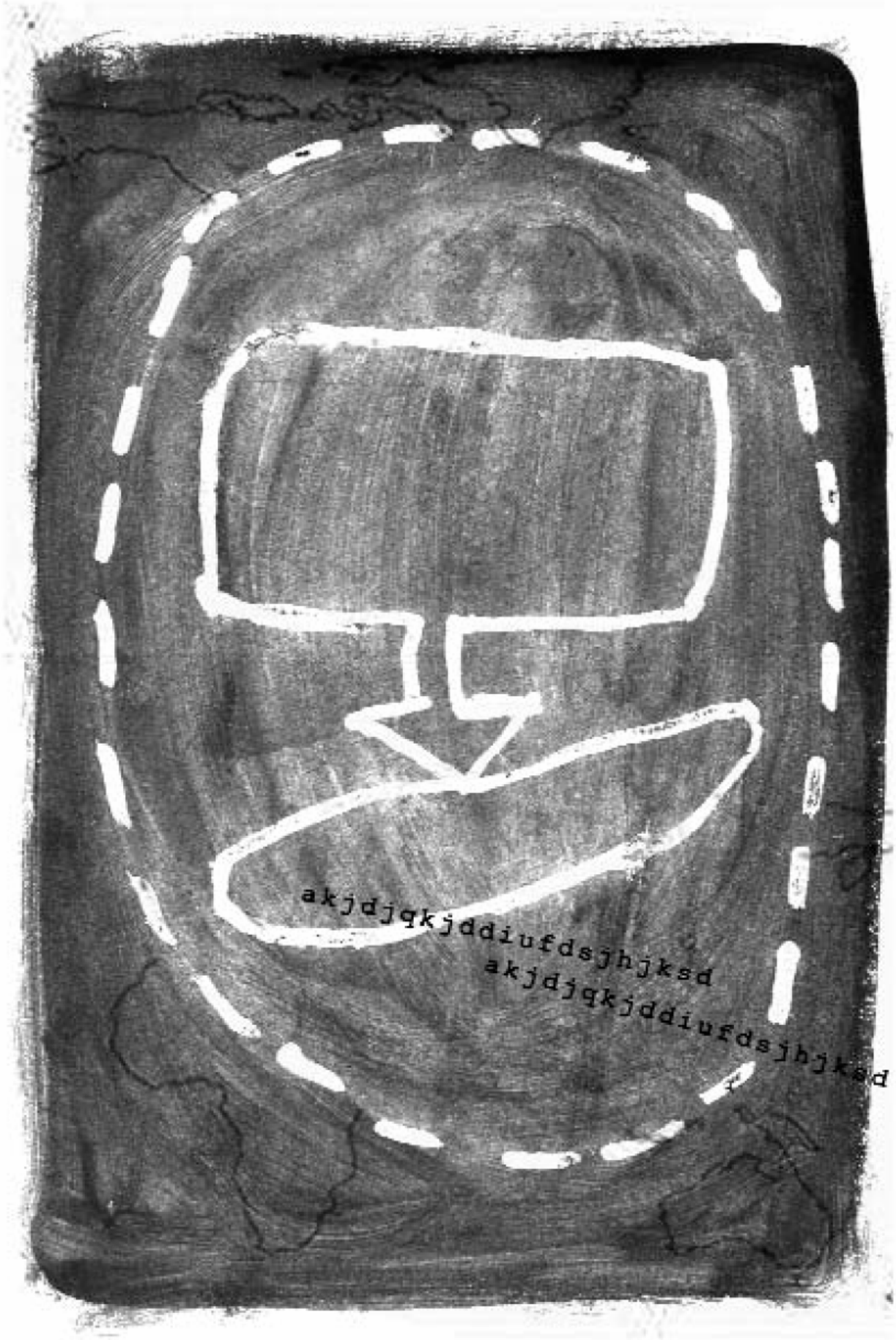
Трэцяя асоба можа замяніць няўзгоднены ключ на фальшывы, тады шыфраваньне згубіць усялякі сэнс. Надзейнасьць асымэтрычнага шыфраваньня цалкам залежыць ад абароны сакрэтнага ключа, а таксама ад праверкі аўтэнтычнасьці адкрытага ключа асобы, зь якой вядзецца ліставаньне.

OpenPGP (Open Pretty Good Privacy) – гэта стандартны спосаб асымэтрычнага шыфраваньня. Найбольш папулярнае праграмнае забесьпячэньне для стварэньня і выкарыстаньня двух ключоў (адкрытага і закрытага), а таксама кіраваньня адкрытымі ключамі тых, хто лістуецца, - гэта GnuPG (GNU Privacy Guard), якое можна выкарыстоўваць як з паштовымі праграмамі (такімі, як Thunderbird і Outlook), так і з уэб-поштай і тэрміновым ліставаньнем.

Праграму GnuPG можна загрузіць з сайта www.gnupg.org

Спэцыяльную вэрсію для Windows можна знайсьці на www.winpt.org

Людовік Пьера – кампутарны інжынэр, узначальвае кампанію "Wa Company", якая займаецца кансультаваньнем і вытворчасьцю ў галіне інфармацыйных тэхналёгій.


akjdjqkjddiufdsjhjksd
akjdjqkjddiufdsjhjksd

КАНТРОЛЬ СЕЦІВА

ЧЭМПІЯНАТ СЬВЕТУ ПА ЦЭНЗУРЫ Ў ІНТЭРНЭЦЕ

Жульен Пэйн (Julien Pain)

Большасьць аўтарытарных рэжымаў імкнецца кантраляваць, што грамадзяне чытаюць і чым займаюцца ў сеціве. Яны ўсё больш пасьпяхова блякуюць "непажаданыя" матэрыялы, звычайна з дапамогай тэхналёгій, набытых у амэрыканскіх кампаній.

У гэтай справе Кітай даўно абыйшоў усіх і стаў сусьветным чэмпіёнам, хоць за апошнія гады ў яго зьявіліся канкурэнты. Кожная з краінаў у нашым, далёка ня поўным сьпісе, мае свой стыль і сваю тактыку, але мэта ў іх адна – абыйсьці праціўніка.

КІТАЙ - ЧЭМПІЁН СЬВЕТУ

Кітай адным з першых рэпрэсіўных рэжымаў зразумеў, што без інтэрнэту не абыйсьціся, і, такім чынам, яго трэба кантраляваць. Кітай – адна зь нямногіх краін, якім удаецца блякаваць усе матэрыялы, што крытыкуюць рэжым, пры адначасовым пашырэньні магчымасьцяў інтэрнэту. Сакрэт – у разумным спалучэньні інвэстыцый, тэхналёгіі і дыпляматыі.

Пэкін выдаткаваў дзесяткі мільёнаў даляраў на самае дасканалае абсталяваньне для ажыцьцяўленьня фільтрацыі і кантролю інтэрнэту. Сыстэма базуецца на чорным сьпісе ўэб-сайтаў, які ўвесь час абнаўляецца. Доступ да "падрыўных" сайтаў (а гэта вельмі шырокі панятак, які ахоплівае парнаграфію, палітычную крытыку, пра-тыбецкія сайты ці сайты, якія заклікаюць да незалежнасьці Тайваня) блякуецца на ўзроўні нацыянальных інтэрнэт-"хрыбтоў" (асноўных вузлоў сувязі). Але на гэтым цэнзура не спыняецца. Рэжым можа аўтаматычна блякаваць доступ да сайтаў, на якіх сустракаюцца "сумнеўныя" ключавыя словы, ці словазлучэньні, як, напрыклад, "цяньаньмынь" + "масавы расстрэл".

Акрамя таго, рэжым можа ажыцьцяўляць амаль імгненную цэнзуру онлайнавых дыскусійных форумаў. Дзякуючы наяўнасьці найноўйшага праграмнага забесьпячэньня, а таксама дзесяткаў тысяч супрацоўнікаў кібэр-паліцыі ўлады кантаралююць онлайнавыя форумы (вельмі папулярныя ў апошнія гады) амаль усіх палітычных дысыдэнтаў. Напрыклад, заклік да свабодных выбараў "пражыве" ў інтэрнэце максімум паўгадзіны. Міністэрства прамысловасьці і інфармацыі таксама сочыць за блогамі, дамовіўшыся пра гэта з блогавымі плятформамі, што базуюцца ў Кітаі. Такім чынам, нататка пра Далай Ламу ў інтэрнэце будзе пярэстая ад прабелаў, аўтаматычна ўстаўленых замест "незаконных" словаў.

Але адкуль у Кітаі такое дасканалае і эфэктыўнае абсталяваньне для ажыцьцяўленьня цэнзуры, калі ўсяго дзесяць год таму ў краіне не было ніводнай буйной інтэрнэт-кампаніі? Адказ: дапамаглі буйныя амэрыканскія кампаніі на чале з Cisco. Для таго, каб завалодаць часткай велічэзнага кітайскага рынку з болей чым 100 мільёнамі карыстальнікаў інтэрнэту, гэтыя кампаніі заплюшчылі вочы на тое, для чаго выкарыстоўваюцца іх тэхналёгіі. Магчыма, некаторыя зь іх супрацоўнічалі з рэжымам і дапамагалі ўсталёўваць фільтры і абсталяваньне для ажыцьцяўленьня кантролю.

Пэкін нават прымусіў да кампрамісу буйнейшыя пошукавыя сыстэмы сьвету. Некалькі год таму Yahoo! пагадзіўся прыбраць са сваёй кітайскай вэрсіі ўсе матэрыялы, якія рэжым лічыць абразьлівымі. Google доўгі час адмаўляўся ад гэтага, але, выглядае, што і ён рухаецца ў тым жа накірунку.

Паліцыя і суды ў Кітаі вельмі сурова абыходзяцца з рэдактарамі сайтаў, якія не падпарадкоўваюцца правілам, прынятым Камуністычнай партыяй, што знаходзіцца ва ўладзе. 75 кібэр-дысыдэнтаў знаходзяцца ў турмах за спробы разьмясьціць у інтэрнэце незалежныя навіны. Некаторыя зь іх асуджаныя на болей за 10 год турэмнага зьняволеньня.

Такім чынам, перш чым распачаць свой блог у Кітаі, азнаёмцеся з парадкамі, якія існуюць у гэтай краіне. Блогерам, што жывуць у краіне, якая зьяўляецца чэмпіёнам цэнзуры інтэрнэту, трэба быць асьцярожнымі і вынаходлівымі.

ВІЕТНАМ: ВЕЛЬМІ МОЦНАЯ КАМАНДА

Віетнам аддана ідзе ўсьлед за Кітаем. Аднак, нягледзячы на тое, што ідэялёгія тут мацнейшая, краіна ня мае эканамічных і тэхналягічных магчымасьцяў, якія ёсьць у суседа. У Віетнаме дзейнічае кібэр-паліцыя, якая адфільтроўвае "падрыўны" матэрыял з уэб-сайтаў і шпіёніць за інтэрнэт-кавярнямі. Але, як і ў Кітаі, яна гэтак жа сурова абыходзіцца з кібэр-дысыдэнтамі і блогерамі, трое зь якіх ужо тры гады знаходзяцца ў турме за тое, што адважыліся выказацца ў інтэрнэце ў падтрымку дэмакратыі.

Прэзыдэнт Зін эль-Абідзін Бэн Алі

ТУНІС: "УЗОРНЫЯ" ГУЛЬЦЫ

Прэзыдэнт Зін эль-Абідзін Бэн Алі, чыя сям'я валодае манаполіяй на інтэрнэт у Тунісе, стварыў вельмі дзейсную сыстэму цэнзуры дзейнасьці ў інтэрнэце. Ён забараніў доступ да ўсіх апазыцыйных сайтаў, а таксама да некаторых сайтаў навінаў, напрыклад, да старонкі французскай газэты "Liberation". Рэжым таксама намагаецца ўпэўніць людзей не карыстацца ўэб-поштай, за якой больш складана сачыць, чым за стандартнымі сыстэмамі электроннай пошты, кшталту Outlook Express. Каб атрымаць доступ да пошты Yahoo! у інтэрнэт-кавярні ў Тунісе можна прачакаць 20 хвілін, да таго ж, чаканьне можа скончыцца атрыманьнем паведамленьня "час выйшаў" ("timed out") ці "старонка ня знойдзеная" ("page not found"). Сайт арганізацыі "Рэпартэры бязь межаў" таксама недаступны ў краіне.

Аднак выглядае, што міжнародная супольнасьць ухваляе тое, як функцыянуе інтэрнэт у Тунісе, паколькі адна са структур ААН – Саюз Міжнародных Тэлекамунікацый (Inernational Telecommunication Union (ITU)) выбраў Туніс месцам правядзеньня Міжнароднай сустрэчы па пытаньнях інфармацыйнага грамадзтва ў лістападзе 2005 году. Ад думкі, што Туніс можа служыць прыкладам разьвіцьця інтэрнэту, робіцца не па сабе.

ІРАН: СУРОВЫЯ МЭТАДЫ

Онлайнавая цэнзура ажыцьцяўляецца ня толькі камуністычнымі рэжымамі ў Азіі. За апошнія гады сыстэмы фільтрацыі ў Іране сталі нашмат больш дасканалымі, і Міністэрства інфармацыі ганарыцца тым, што блякуе доступ да соцень тысяч уэб-сайтаў. Муллы загадваюць фільтраваць, у першую чаргу, любую інфармацыю пра сэкс, а таксама сайты зь незалежнымі навінамі.

Рэжым Ірана, здольны на самыя жорсткія мэтады цэнзуры, паставіў свайго роду рэкорд, калі ў 2005 годзе на працягу 10 месяцаў амаль 20 блогераў былі кінутыя ў турмы. На 1 жніўня 2005 году трое зь іх усё яшчэ заставаліся за кратамі.

прэзыдэнт Фідэль Кастра

КУБА: "ЛЕГЕНДА"

Кубінскі рэжым добра вядомы праслухоўваньнем тэлефонных размоваў, але і фільтрацыя інтэрнэту ў яго таксама добра атрымліваецца. Кітайская мадэль заахвочваньня дзейнасьці ў інтэрнэце з адначасовым кантролем за гэтай дзейнасьцю занадта дарагая, таму прэзыдэнт Фідэль Кастра выбраў лягчэйшы шлях – проста зрабіў інтэрнэт недаступным фактычна для ўсіх кубінцаў. Прывілею карыстацца інтэрнэтам на Кубе маюць нямногія. Для гэтага неабходна атрымаць дазвол Камуністычнай партыі, што кіруе краінай. Нават калі хтосьці і мае доступ да інтэрнэту (часьцей за ўсё, незаконна), то гэта вельмі моцна цэнзураваная вэрсія.

Мала хто ведае, што Куба – адна з краін зь мінімальным выкарыстаньнем інтэрнэту ў сьвеце, і што ў дачыненьні да інтэрнэту тут выкарыстоўваецца такая ж моцная цэнзура, як і да традыцыных сродкаў масавай інфармацыі. Чаму людзі гэтага ня ведаюць? Магчыма, таму, што дагэтуль знаходзяцца пад узьдзеяннем міту пра кубінскую рэвалюцыю.

Кароль Абдаллах Бен Абдэль Азіз аль-Сауд

САУДАЎСКАЯ АРАБІЯ: РЭКОРДНЫЯ ДАСЯГНЕНЬНІ

Улады Саудаўскай Арабіі адкрыта заяўляюць пра тое, што ажыцьцяўляюць фільтрацыю інтэрнэту. Ніякіх паведамленьняў "старонка ня знойдзеная", як у Кітаі. Калі вы паспрабуеце зайсьці на забаронены сайт, адразу ж атрымаеце паведамленьне, што сайт заблякаваны фільтрамі ў адпаведнасьці з загадам ўрада краіны. Афіцыйная структура, якая займаецца пытаньнямі інтэрнэту (Internet Service Unit (ISU)) з гонарам паведаміць, што ўжо заблякавала каля 400 000 сайтаў, а таксама разьмясьціла ў інтэрнэце форму для карыстальнікаў, у якую можна ўпісаць сайты, якія, на думку гэтых карыстальнікаў, трэба заблякаваць. ISU лічыць, што фільтруе сайты, каб абараніць грамадзян ад інфармацыі, якая зьневажае прынцыпы ісламу і парушае сацыяльныя нормы.

Цікавая інфармацыя: амэрыканская кампанія "Secure Computing" прадала ўладам Саудаўскай Арабіі сваю сыстэму онлайнавай фільтрацыі.

УЗБЭКІСТАН: МАЙСТРЫ БЛЕФУ

"У нашай краіне няма цэнзуры інтэрнэту",- заявіў у чэрвені 2005 году міністар інфармацыі Узбэкістану. Гэтая заява гучыць вельмі дзіўна, улічваючы, што ў краіне няма доступу да ніводнага апазыцыйнага ўэб-сайта, а інтэрнэт-журналістам пагражаюць, і яны робяцца ахвярамі фізічнага насільля.

Жульен Пэйн – кіраўнік праекту "Свабода ў інтэрнэце" ў арганізацыі "Рэпартэры бязь межаў".

“РЭПАРТЭРЫ БЯЗЬ МЕЖАЎ”
REPORTERS WITHOUT BORDERS

Міжнародны сакратарыят
5, rue Geoffroy-Marie, 75009 Paris, France
Tel.: 33 1 4483-8484
Fax.: 33 1 4523-1151

Уэб-сайт: **www.rsf.org**

Рэдактар: Сільві Дэвілет (Sylvie Devilette)
Кантакты: Эн Марцінез-Сэз (Anne Martinez-Saiz / communication@rsf.org)
Графічны дызайн і ілюстрацыі: (NDC) Nuit de Chine ndc@nuitdechine.com

ISBN: 2-915536-36-8
Аўтарскае права: арганізацыя “Рэпартэры бязь межаў” 2005
Copyright: Reporters sans frontieres 2005